Guidance Software

EnCase Legal Journal

Second Edition

Preface

Computer forensics is a discipline dedicated to the collection of computer evidence for judicial purposes. Those who practice computer forensics should be very familiar with the laws of evidence in their relevant jurisdictions so that they may correctly employ the proper procedures, tools and methodologies used to collect and process computer evidence. While there has been some excellent research and writing on search and seizure and privacy issues related to computer data, there has been comparatively little guidance on the authentication and presentation of electronic evidence at trial.

Computer investigation experts uncertain of what the law required often received unclear direction from counsel who were equally unfamiliar with the complex technical issues and nuances that must be applied to the laws of evidence. Consequently, there has been no clear consensus on issues such as what is required to establish a sufficient foundation for computer evidence, whether a computer forensic investigator is considered a scientific expert, and how the Best Evidence rule applies to computer data.

In response to these concerns, Guidance Software launched The EnCase Legal Journal ("ELJ"), which is provided with two goals in mind. First, the ELJ reports on recent trial court developments involving EnCase as well as notable court decisions involving computer evidence in general. Secondly, the ELJ addresses how the EnCase process facilitates the authentication and admission of electronic evidence in light of past industry practices and the current status of the law, providing investigators and their counsel with an added resource when addressing questions involving computer forensics and the use of EnCase.

The ELJ is provided for informational purposes and is not intended as legal advice and should not be construed or relied upon as such. Each set of circumstances may be different and all cited legal authorities should be confirmed and updated.

Just as Guidance Software is committed to ongoing product research and development, so must we also be on top of the latest legal developments impacting this field. As such, this journal should be considered as a work perpetually in progress. If you have any questions, comments or suggestions for future revisions, please feel free to contact me at John.Patzakis@EnCase.com.

John Patzakis
Guidance Software
June 2001

Table of Contents

1

Authentication of Computer Evidence

§1.0 Overview

Documents and writings must be authenticated before they may be introduced into evidence. The US Federal Rules of Evidence, as well as the laws of many other jurisdictions, define computer data as documents.[1] Electronic evidence presents particular challenges for authentication as such data can be easily altered without proper handling. The proponent of evidence normally carries the burden of offering sufficient evidence to authenticate documents or writings, and electronic evidence is no exception.

What testimony is required to authenticate computer data? How does a witness establish that the data he or she recovered from a hard drive is not only genuine but completely accurate? Are there guidelines or checklists that should be followed? How familiar with the software used in the investigation must the examiner be in order to establish a proper foundation for the recovered data? These are some of the questions that face computer investigators and counsel when seeking to introduce electronic evidence. This chapter will address these questions.

§1.1 Authentication of Computer Data

Oftentimes, the admission of computer evidence, typically in the form of active ("non-deleted") text or graphical image files, is accomplished without the use of specialized computer forensic software. Federal Rule of Evidence 901(a) provides that the authentication of a document "satisfied by evidence sufficient to support a finding that the matter in question is what the proponent claims." The Canada Evidence Act specifically addresses the authentication of computer evidence, providing that an electronic document can be authenticated "by evidence capable of supporting a finding that the electronic document is that which it is purported to be."[2] Under these statutes, a printout of an e-mail message can often be authenticated simply through direct testimony from the recipient or the author.[3]

The US Federal Courts have thus far addressed the authentication of computer-generated evidence based upon Rule 901(a), much in the same manner as statutes that have existed before computer usage became widespread.[4] *United States v. Tank,*[5] which involves evidence of Internet chat room conversation logs, is an important illustration.

In *Tank*, the Defendant appealed from his convictions for conspiring to engage in the receipt and distribution of sexually explicit images of children and other offenses. Among the issues addressed on appeal was whether the government made an adequate foundational showing of the relevance and the authenticity of a co-conspirator's Internet

chat room log printouts. A search of a computer belonging to one of Defendant Tank's co-conspirators, Riva, revealed computer text files containing "recorded" online chat room discussions that took place among members of the Orchard Club, an Internet chat room group to which Tank and Riva belonged.[6] Riva's computer was programmed to save all of the conversations among Orchid Club members as text files whenever he was online.

At an evidentiary hearing, Tank argued that the district court should not admit the chat room logs into evidence because the government failed to establish a sufficient foundation. Tank contended that the chat room log printouts should not be entered into evidence because: (1) they were not complete documents, and (2) undetectable "material alterations," such as changes in either the substance or the names appearing in the chat room logs, could have been made by Riva prior to the government's seizure of his computer.[7] The district court ruled that Tank's objection went to the evidentiary weight of the logs rather than to their admissibility, and allowed the logs into evidence. Tank appealed, and the appellate court addressed the issue of whether the government established a sufficient foundation for the chat room logs.

The appellate court considered the issue in the context of Federal Rule of Evidence 901(a), noting that "[t]he rule requires only that the court admit evidence if sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity or identification . . . The government must also establish a connection between the proffered evidence and the defendant."[8]

In authenticating the chat room text files, the prosecution presented testimony from Tank's co-conspirator Riva, who explained how he created the logs with his computer and stated that the printouts appeared to be an accurate representation of the chat room conversations among members of the Orchid Club. The government also established a connection between Tank and the chat room log printouts. Tank admitted that he used the screen name "Cessna" when he participated in one of the conversations recorded in the chat room log printouts. Additionally, several co-conspirators testified that Tank used the chat room screen name "Cessna" that appeared throughout the printouts. They further testified that when they arranged a meeting with the person who used the screen name "Cessna," it was Tank who showed up.[9]

Based upon these facts, the court found that the government made an adequate foundational showing of the authenticity of the chat room log printouts under Rule 901(a). Specifically, the government "presented evidence sufficient to allow a reasonable juror to find that the chat room log printouts were authenticated."[10]

The *Tank* decision is consistent with other cases that have addressed the issue of the authenticity of computer evidence in the general context of Fed.R.Evid. 901(a).[11] *Tank* illustrates that there are no specific requirements or set procedures for the authentication of chat room conversation logs, but that the facts and circumstances of the creation and recovery of the evidence as applied to Rule 901(a) is the approach generally favored by the courts. (See also *United States v. Scott-Emuakpor,*[12] [Government

properly authenticated documents recovered from a computer forensic examination under Rule 901(a)]).

§1.2 Authentication of the Recovery Process

Where direct testimony is not available, a document may be authenticated through circumstantial evidence. A computer forensic examination is often an effective means to authenticate electronic evidence through circumstantial evidence. The examiner must be able to provide competent and sufficient testimony to connect the recovered data to the matter in question.

Courts have recognized the importance of computer forensic investigations to authenticate computer evidence. *Gates Rubber Co. v. Bando Chemical Indus., Ltd.,*[13] is a particularly important published decision involving competing computer forensic expert testimony, where the court essentially defines a mandatory legal duty on the part of litigants or potential litigants to perform proper computer forensic investigations. There, one party's examiner failed to make a mirror image copy of the target hard drive and instead performed a "file-by-file" copy in an invasive manner, resulting in lost information.[14] The opposing expert noted that the technology needed for a mirror image backup was available at the time (February 1992), even though not widely used. In its ruling issuing harsh evidentiary sanctions, the court criticized the errant examiner for failing to make an image copy of the target drive, finding that when processing evidence for judicial purposes a party has "a duty to utilize the method which would yield the most complete and accurate results."[15]

Some courts have required only minimal testimony concerning the recovery process, particularly where the defense fails to raise significant or adequate objections to the admission of the computer evidence. In *United Sates v. Whitaker*[16] an FBI agent obtained a printout of business records from a suspect's computer by simply operating the computer, installing Microsoft Money and printing the records.[17] The court affirmed the admission of the printouts, finding that testimony of the agent with personal knowledge of the process used to retrieve and print the data provided sufficient authentication of the records.[18] However, in an apparent admonition to the defense bar, the court noted that the defense conspicuously failed to question the FBI agent "about how the disks were formatted, what type of computer was used, or any other questions of a technical nature."[19]

Other cases have involved more extensive objections to computer-based evidence. *People v. Lugashi*[20] is a particularly notable case involving a detailed analysis by the court on this subject. Although not involving a computer forensic investigation per se, the Court addressed issues concerning the authentication of computer-based evidence challenged by the defense in a criminal prosecution. *Lugashi* involved a credit card fraud investigation, where a bank's internal computer system recorded and stored relevant data relating to a series of transactions in question. Each night, the bank's computer systems ran a program known as a "data dump," which retrieved and organized the daily credit card transactions reported to the bank. Shortly thereafter, a backup tape was made of the

"dump" from which a microfiche record was prepared and maintained.[21]

The prosecution sought to introduce the computer-generated evidence generated by this process largely through the testimony of one of the bank's systems administrators, who conceded that she was not a computer expert. She did, however, work with those who ran the "data dumps," maintained the microfiche records, and was familiar with the system. She personally produced the data in question from the microfiche records and knew how to interpret it.[22] The defense contended that as the systems administrator was not a computer expert she was incompetent to authenticate the data in question and that, essentially, only the computer programmers involved in the design and operation of the bank's computer systems could adequately establish that the systems and programs in question were reliable and free from error. The defense also asserted that because the systems administrator's understanding of how the system worked came from her discussions with the bank's programmers and other technical staff, her testimony constituted hearsay and thus should not be allowed.[23]

The court rejected the defense's argument, noting that the defense's position incorrectly assumed that only a computer expert "who could personally perform the programming, inspect and maintain the software and hardware, and compare competing products, could supply the required testimony."[24] Instead the court ruled that "a person who generally understands the system's operation and possesses sufficient knowledge and skill to properly use the system and explain the resultant data, even if unable to perform every task from initial design and programming to final printout, is a 'qualified witness'" for purposes of establishing a foundation for the computer evidence.[25] The court noted that if the defense's proposed test were applied to conventional hand-entered accounting records, for example, the proposal "would require not only the testimony of the bookkeeper records custodian, but that of an expert in accounting theory that the particular system employed, if properly applied, would yield accurate and relevant information."[26] Further, if the defense's position were correct, "only the original hardware and software designers could testify since everyone else necessarily could understand the system only through hearsay." The *Lugashi* court also commented that the Defense's proposed test would require production of "hordes" of technical witnesses that would unduly burden both the already crowded trial courts and the business employing such technical witnesses "to no real benefit."[27]

It should be noted that there are some factors and aspects of the *Lugashi* decision that may not be completely applicable to computer forensics. For instance, *Lugashi* deals with records created in the normal course of business, which courts in the United States generally presume to be authentic, subject to the presentation of any direct evidence to the contrary. Further, a disinterested third party to the litigation generated the computer records in *Lugashi*, while courts would likely apply increased scrutiny to records generated by a law enforcement investigator or retained party expert. However, certain aspects the *Lugashi* decision seem applicable to questions regarding what is required to establish a proper foundation for evidence obtained from a computer forensic examination. (See also *Federal Deposit Insurance Corporation v. Carabetta*[28] [similar facts and holding to *Lugashi]*).

In addition to the citations provided throughout this text relating to the admission of recovered computer data, other court rulings concerning various forms of electronic evidence provide additional and important insight regarding what many courts require for establishing a proper foundation for such data. Many of these cases frame the same issues as to what extent the investigator must be familiar with the process used to obtain or generate the electronic evidence.

Bray v. Bi-State Development Corp.[29] addressed whether an expert's testimony provided a sufficient foundation to establish the validity of computer software that produced a chart depicting light intensity levels to determine adequate lighting for commercial areas. The software program utilized photometric data to accurately calculate light intensity based on general parameters and inputted data. The expert testified that he was familiar with the software and its general functionality and that the program was known to produce accurate results and was generally used by lighting manufacturer representatives and lighting engineers. He also testified that while he had personal knowledge of the data that was inputted into the program, he generally relied on the manufacturer's representative to actually operate the computer.[30] The objecting party contended that the expert failed to establish a sufficient foundation because the expert did not program the computer software, did not actually operate the program in question, and offered no specific evidence that the software was accurate or reliable.

The court in its opinion determined that the "[r]elevant technical or scientific community's use of or reliance on particular computer software is sufficient to establish accuracy of that software for purposes of admissibility of computer-generated evidence."[31] The court also noted *Federal Rule of Evidence* 901(b)(9) and ultimately relied on both concepts in its ruling, finding testimony that the "software was a program which produced accurate results and was used generally by the lighting manufacturer's representative and relied on by engineers to design light and make lighting decisions was sufficient under these circumstances."[32]

In *State of Arizona v. Rivers,*[33] the Defendant's terms of parole subjected him to electronic monitoring to verify compliance with his house arrest. The monitoring equipment included an ankle-bracelet transmitter and a receiver connected to the defendant's telephone. The receiver was programmed with the defendant's schedule and was designed to automatically notify a parole office computer if the defendant left his home or failed to return to his home during curfew hours.[34] After the monitoring equipment detected multiple curfew violations, the defendant was apprehended and charged with various parole violations. At trial, the defendant argued that because the parole officers were not qualified to testify "from a scientific standpoint" about how the subject monitoring equipment functioned, the state was unable to demonstrate that the equipment was in proper working condition when it registered his failure to return home. The parole officer acknowledged that he did not consider himself to be an "expert" on how the monitoring equipment worked, but did testify that he had worked with approximately 200 to 300 parolees on home arrest and that he did not recall ever having received incorrect information from the equipment. He told the jury that, to the best of his

knowledge, the equipment was working properly when it registered the defendant's failure to return on the day in question.[35] Based upon this testimony, the trial court ruled that the state established a sufficient foundation for the electronic evidence of curfew violations.

On appeal, the appellate court found no error in the trial court's conclusion that the state provided sufficient foundation and evidence from which the jurors could reasonably conclude that the monitoring equipment was functioning properly when it registered the defendant's curfew violation. The court cited key testimony provided by the parole officers concerning the equipment's general accuracy and reliability. Additionally, the court noted that the officers testified that the equipment was correctly installed and in proper working condition on the date in question.[36] The court relied on the case of *Ly v. State of Texas,*[37] which involved a nearly identical fact scenario, and where that court similarly rejected a defendant's contention that because the government witness was not familiar with the scientific principles behind the electronic-monitoring equipment, the state could not demonstrate that the equipment was reliable and that it had worked properly in his case.

In *United States v. Sanchez,*[38] the defendants contended that the government failed to establish that a forward-looking infrared device ("FLIR") attached to a surveillance aircraft was functioning properly when a United States Customs agent observed an aircraft engage in a night-time delivery of narcotics on a remote airstrip. Specifically, the defendants argued that because the agent admitted that he was not an expert in how the FLIR worked, the government had failed to demonstrate that the device functioned properly, and thus the testimony was insufficient to lay a proper foundation for introduction of the evidence obtained through the use of the FLIR. Rejecting the defendants' argument, the court concluded that the agent's "significant experience as a pilot in a FLIR-equipped plane" was sufficient to enable him to testify that the device "appeared to be functioning properly" at the time.[39] The court also noted that the agent was able to describe the basic principles upon which the FLIR operated. Thus, the trial court did not abuse its discretion in admitting the agent's testimony concerning the events viewed through the FLIR.

These cases demonstrate that when addressing proper foundation for electronic evidence generated by complex devices or software, the courts generally apply the same analysis of "sufficient familiarly" by the user, general acceptance, and whether the process involved is standard and commercially available. The general acceptance standard, which is more fully addressed in the next chapter, is clearly a predominant consideration. Additionally, whether the expert is experienced and/or trained in the software and process involved is also important consideration.

However, while experience and proper training are clearly important, it is also clear that the courts do not mandate that the expert be intimately familiar with the scientific principles or detailed inner workings of these technical processes that generate electronic evidence.

§1.3 Authentication of the EnCase Recovery Process

Under the standard articulated under *Lugashi* and several other similar cases, the examiner need not be able to intricately explain how each and every function of EnCase works in order to provide sufficient testimony regarding the EnCase process. There are no known authorities requiring otherwise for software that is both commercially available and generally accepted. A skilled and trained examiner with a strong familiarity with the EnCase process should be able to competently present EnCase-based evidence obtained through a forensic examination.[40]

An examiner should have a strong working familiarity of how the program is used and what the EnCase process involves when seeking to introduce evidence recovered by the program. This means that the examiner should ideally have received training on EnCase, although such training should not be strictly required, especially where the witness is an experienced computer forensic investigator and has received computer forensic training on computer systems in the past. Examiners should also conduct their own testing and validation of the software to confirm that the program functions as advertised. However, a "strong working familiarity" does not mean that an examiner must obtain and be able to decipher all 300,000 lines of the program source code or be able to essentially reverse engineer the program on the witness stand.

§1.4 Challenges to Foundation Must Have Foundation

In the event the initial evidentiary foundation established by the computer forensic examiner's testimony is sufficiently rebutted, so as to challenge the admissibility or the weight of the evidence, expert testimony to, in turn, rebut such contentions may be required. However, courts will normally disallow challenges to the authenticity of computer-based evidence absent a specific showing that the computer data in question may not be accurate or genuine—mere speculation and unsupported theories generally will not suffice.[41] There is ample precedent reflecting that unsupported claims of possible tampering or overlooked exculpatory data are both relatively common and met with considerable skepticism by the courts. One federal court refused to consider allegations of tampering that was "almost wild-eyed speculation . . . [without] evidence to support such a scenario." Another court noted that the mere possibility that computer data could have been altered computer data is "plainly insufficient to establish untrustworthiness."[42]

One court suggests that the defense should perform its own credible computer forensic examination to support any allegation of overlooked exculpatory evidence or tampering.[43] Another court noted that while some unidentified data may have been inadvertently altered during the course of an exam, the defendant failed to establish how such alteration, even if true, affected the data actually relevant to the case.[44] As such, in order for a court to even allow a challenge based upon alleged tampering or alteration of the computer data, the defense should be required to establish both specific evidence of alteration or tampering and that such alteration affected data actually relevant to the case. Further, even if some basis to allegations that relevant computer records have been altered, such evidence would go to the weight of the evidence, not its admissibility. [45]

2

Validation of Computer Forensic Tools

§ 2.0 Overview

Chapter 1 addressed authenticating computer evidence through direct or circumstantial evidence in order to establish that the recovered data is genuine and accurate. Another form of an objection to authenticity may involve questioning the reliability of the computer program that generated or processed the computer evidence in question. In such cases, the proponent of the evidence must testify to the validity of the program or programs utilized in the process. This chapter discusses what standards the courts are actually applying in such challenges, and what testimony the examiner may need to provide to validate computer forensic tools.

§ 2.1 *Frye/Daubert* Standard

Daubert v. Merrell Dow Pharmaceuticals, Inc,[46] is an important federal court decision that sets forth a legal test to determine the validity of scientific evidence and its relevance to the case at issue. Many state court jurisdictions in the US follow the *Frye*[47] test, which is very similar, but not identical to *Daubert.* The introduction of DNA evidence is a typical scenario where a court may require a *Daubert/Frye* analysis, although many courts now take judicial notice of the accuracy of DNA typing procedures as the science is no longer considered "novel."[48]

We have seen *Daubert/Frye* raised in most all concerted challenges to EnCase. However, a corporate defendant advocating the EnCase-based evidence in *Mathew Dickey v. Steris Corporation*[49] (further discussed at §6.01) successfully asserted that EnCase constituted an automated process that produces accurate results, and thus evidence obtained from that process would be subject to a presumption of authenticity under Rule 901(b)(9). Rule 901(b)(9) provides that evidence produced by an automated process, including computer-generated evidence, may be authenticated if such an automated process is shown to produce accurate results. However, the court also addressed the *Daubert* factors. Although it is clear that EnCase meets both the standards under both Rule 901 and *Daubert*,[50] the recent trend of the courts is to include "non-scientific" technical evidence within the purview of *Daubert/Frye*, in addition to the purely scientific forms of evidence, such as DNA analysis, that are more traditionally subject to *Daubert*. The judicial analysis applied in recent notable challenges to EnCase is clearly consistent with this trend. As such, a computer forensic examiner should be very familiar with the basic elements of the *Daubert* analysis, which are as follows:

1) Whether a "theory or technique … can be (and has been) tested;"

2) Whether it "has been subjected to peer review and publication;"
3) Whether, in respect to a particular technique, there is a high "known or potential rate of error;" and
4) Whether the theory or technique enjoys "general acceptance" within the "relevant scientific community."[51]

Under the first prong of the test, courts have expressly noted that EnCase is a commercially available program that can be easily tested and validated. This is in contrast to tools that are not commercially available to the general public or are custom tools with arcane command line functionality that are not easily tested by third parties unfamiliar with those processes. The law is clear that in the context of computer-generated evidence, the courts favor commercially available and standard software.[52] Further, many agencies have tested EnCase in their labs before standardizing their agents with the software. Importantly, the widespread adoption of EnCase by the computer forensics community serves as a crucial factor for authentication, as the community generally knows the capabilities and accuracy of the program through such extensive usage. Additionally, recent publications have featured EnCase as the highest-rated tool in testing and comparisons among other commercially available software tools.[53]

These reviews are among several industry publications featuring EnCase, and are relevant to the second prong of the *Daubert* test. Peer review and publication in the relevant industry is an important factor looked to by the Courts in considering the validity of a technical process under *Daubert/Frye*. Various published articles in the information security and high-tech crime investigation industries favorably review or mention EnCase favorably.[54] Among the more notable articles is the recent IEEE Computer Society publication, *Computer Magazine*, which featured a "case study" of the EnCase technology and reported on its widespread use and acceptance in the computer forensics community. It is important for computer forensic examiners to keep abreast of peer review of computer forensic tools in industry publications. Examiners should also be cognizant of whether developers decline invitations from respected industry publications to participate in testing and peer review opportunities, as such refusals could raise questions regarding the validity of such tools.

It is not uncommon for investigators to be asked to testify to specific examples of peer review and publication of technical or scientific processes. For instance, in *People v. Rodriguez,*[55] a recent case in Sonoma County, California where EnCase was subjected to a *Frye* analysis, the District Attorney investigator referenced in his testimony the above-mentioned IEEE Computer Society article and others currently available in the Newswire section of the Guidance Software website. Often, testifying experts will bring copies of relevant articles from industry publications to court for admission into evidence as part of the validation process.

The prosecution in *Rodriguez* also provided testimony that there were no known reports of a high known or potential rate of error regarding EnCase. While all software programs contain bugs to varying degrees, the various tests and extensive usage of EnCase reveal that the program does not have a high error rate, especially in contrast to

other available tools. Additionally, it is important for an investigator to be able to point to either his/her own testing of EnCase or that performed by his/her agency. In the most detailed and documented published testing results of computer forensic software to date, *SC Magazine* notes that EnCase "outperformed all the other tools" that were tested by the magazine.[56]

Courts have referred to the need for a body of data from "meaningful testing" efforts to guide them in their *Daubert* analysis. There is no requirement for a rigorous and universal standard for such testing agreed on by all the experts in the field. However, any testing should be meaningful and objective, subject to the same peer review as the tools and processes being analyzed. Further, professional testing ideally culminates in the preparation of a detailed report or white paper, allowing for proper analysis and comment.

Because computer forensics remains a relatively new field, there is not an ideal amount of published testing. Many large agencies have conducted successful tests with EnCase but have not published their results. Additionally, it is difficult to determine whether a particular tool has a high rate of error unless the testing process and methodologies are disclosed and documented in full. It is also difficult to define a "high rate of error" when many developers of popular forensic tools decline to allow testing on their tools, depriving the analysis of a wider field of comparison. However, as this industry matures, the amount of documented and objective testing should increase substantially.

The final prong — whether a process enjoys "general acceptance" within the "relevant scientific community" — is a particularly important factor strongly considered by the courts in validating scientific tools and processes. "`[A] known technique that has been able to attract only minimal support within the community,' ... may properly be viewed with skepticism."[57] EnCase is without question the most widely used computer forensic process in the field. Over three thousand law enforcement agencies and companies worldwide employ EnCase for their computer investigations. The widespread general acceptance of a process is often considered to be the most important prong in a *Daubert/Frye* analysis.

In the case of many other technical processes, counsel will often struggle to establish that all the *Daubert* factors are sufficiently met. However, it is difficult to imagine any other computer forensic process that could better qualify under the *Daubert/Frye* analysis. In fact, at least one trial court has taken official judicial notice that EnCase is a commercially available tool with widespread general acceptance.[58] Counsel should consider seeking judicial notice from the court of several of the *Daubert* factors as applied to EnCase, including its general acceptance, the fact that is commercially available and subject to widespread peer review.[59]

§ 2.2 Computer Forensics as an Automated Process

Federal Rule of Evidence 901(b)(9) provides a presumption of authenticity to evidence generated by or resulting from a largely automated process or system that is shown to produce an accurate result. This rule is often cited in the context of computer-processed evidence.[60] There is some debate as to whether testimony from computer forensic examiners should be considered expert scientific testimony, and thus subject to an analysis under *Daubert*, or non-scientific technical testimony regarding the recovery of data through a technical investigation process, and thus subject to Federal Rule of Evidence 901(a), 901(b)(9). The United States Supreme Court blurred this distinction between scientific vs. non-scientific expert testimony in its *Kumho Tire Company, Ltd. v. Carmichael*,[61] which extended the *Daubert* test to cover technical processes as well as scientific opinion evidence. However, many courts still draw a general distinction between scientific and non-scientific expert testimony.[62]

At least one federal appeals case has referred to this issue in *dicta*, hypothesizing that in light of Rule 901(b)(9), computer or x-ray evidence resulting from a process or system would not fall under a *Frye* analysis as "[t]he underlying principles behind x-ray and computers are well understood; as to these technologies, serious questions of accuracy and reliability arise, if at all, only in connection with their application in a particular instance."[63] The court in *United States v. Whitaker*,[64] held that, without addressing *Daubert,* a foundation for forensically recovered computer evidence could be established by the investigating agent with personal knowledge of the process used to retrieve and print the data.[65]

In *United States v. Quinn,*[66] the prosecution sought to introduce "photogrammetry" evidence through expert testimony to determine the height of a suspect from surveillance photographs. The trial court allowed the testimony after a simple proffer from the government as to the basis of a photogrammetry process, which the court found to be "nothing more than a series of computer-assisted calculations that did not involve any novel or questionable scientific technique."[67] The court of appeal rejected the defendant's contention that the photogrammetric evidence required an evidentiary hearing under *Daubert*, finding that the trial court acted within its discretion.[68] In *Burleson v. State,*[69] the court held that expert testimony resulting from a complicated computer-generated display showing deleted records was admissible, as the software and computer systems creating the output relied upon by the expert were shown to be standard, accurate and reliable. The court noted that it was unnecessary for the computer system technology to be authenticated under a *Frye* test, finding that the showing of an accurate and reliable system producing the display was sufficient.[70]

EnCase is proven to provide a more accurate, objective and complete search and recovery process through a substantially automated process. In more complex computer forensic cases, evidence concerning the search and recovery function with its resulting visual outputs and printed reports is often as important as the recovered data itself. Some tools exclusively employed by a minority of computer forensics examiners are little more than basic single-function DOS disk utilities that, when combined as a non-integrated suite, are manipulated to perform computer forensic applications. This formerly common

practice presents three fundamental problems: 1) results from the examiner's search and recovery process are often subjective, incomplete and variant; 2) the data restoration process can either improperly alter the evidence on the evidentiary image copy or provide a visual output that is not a complete and accurate reflection of the data contained on the target media; and 3) the lack of integration of all essential forensic functions within a single software application presents potential challenges to the authenticity of the processed computer evidence.

Applying Rule 901(b)(9) to the context of electronic data discovery, computer forensic software should ideally provide an objective and automated search and data restoration process that facilitate consistency and accuracy. To provide a hypothetical illustration, a group of ten qualified and independently operating forensic examiners analyzing the same evidentiary image should achieve virtually the same search results when entering identical text search keywords or seeking to recover all specified file types on the image, such as all graphical images or all spreadsheet files. If not, the process employed cannot be considered to be either automated or accurate and thus would not be considered a process qualifying for a presumption of authenticity under Rule 901(b)(9). Further, it is often necessary to duplicate search processing results during or before trial, and thus if a colleague or, even worse, an opposing expert obtains significantly differing search results from the same media, the impact or even the very foundation of the evidence may be substantially weakened. While the court in *Gates Rubber* did not expressly cite Rule 901(b)(9), its holding that a computer examiner has "a duty to utilize the method which would yield the most complete and accurate results" is clearly consistent with the statute.

Results from search and recovery procedures utilizing DOS utilities will significantly vary depending upon the type and sequence of non-integrated utilities employed, the amount of media to be searched, and the skill, biases and time availability of the examiner. Further, each piece of acquired media must be searched separately, using the same tedious and time consuming protocol for each hard drive, floppy disk, CD or other media involved in the case. In sum, the likelihood of different independently operating examiners duplicating the search and restoration process on the same evidentiary image is extremely remote, if not impossible.

Due to the inordinate burden of searching a Windows image with DOS utilities, some investigators resort to operating Windows Explorer on the evidentiary image disk. In addition to not being able to view file slack, swap files and all other types of unallocated data, Explorer will corrupt the data in such a situation by altering file date stamps, temporary files and other transient information. Better practice requires specially designed Windows-based computer forensic software that employs a completely non-invasive and largely automated search process. A more objective search process facilitates results that are dramatically more accurate and consistent, thereby enabling duplication of the process at trial and by independently operating examiners. For example, when utilizing EnCase, simply clicking a request to display all graphical image files contained on an evidentiary image disk will instantaneously list all such files in a graphical interface, including files "re-named" or hidden in obscure directories by a

suspect in order to conceal them, and even, in most cases, previously deleted files. EnCase duplicates the Windows Explorer interface and viewing functions, with the critical added benefits of viewing deleted files and all other unallocated data in a completely non-invasive manner. An EnCase search process often reduces an examiner's lab analysis time by several weeks. Most importantly, an examiner can present the discovered evidence in court with confidence that the search and recovery process provided more complete, consistent and objective results.

It should be noted that the line of cases that applied rule 901(a)(b) discussed above preceded *Kumho Tire*, which, as also noted above, extended the *Daubert* test to technical processes as well as scientific opinion evidence. EnCase has been authenticated at trial under both *Daubert/Frye* and Rule 901(b)(9), and it is advisable that both approaches be considered in authenticating the software.

§ 2.3 Commercial vs. Custom Forensic Software and Authentication Issues

Some computer forensic investigations utilize custom software tools developed by the investigating agency or a private company that are not commercially available to the general public. Courts have addressed issues concerning the type of software involved where computer-generated evidence is at issue. Such cases provide a presumption of authenticity for evidence resulting from or processed by commercially available computer systems and software over customized systems and software. As noted by one respected treatise on the subject:

> "Evidence generated through the use of standard, generally available software is easier to admit than evidence generated with custom software. The reason lies in the fact that the capabilities of commercially marketed software packages are well known and cannot normally be manipulated to produce aberrant results. Custom software, on the other hand, must be carefully analyzed by an expert programmer to ensure that the evidence being generated by the computer is in reality what it appears to be. Nonstandard or custom software can be made to do a host of things that would be undetectable to anyone except the most highly trained programmer who can break down the program using source codes and verify that the program operates as represented."[71]

In fact, courts in many jurisdictions actually require that any computer-generated evidence be a product of a "standard" computer program or system in order to admit such evidence.[72] This body of authority would seem especially relevant to software used by law enforcement for computer forensic purposes, given the sensitive function of such software. A law enforcement agency that utilized customized proprietary software for computer forensic investigations could face various complications when seeking to introduce evidence processed with such software. Such actual or potential pitfalls could include the following:

1. The defense could seek to exclude the results of any computer investigation that utilized tools that were inaccessible to non-law enforcement. Federal courts are unanimous in holding that computer evidence generated by or resulting from a process is only admissible if the defense has access to such software in order to independently duplicate the results of that process and thus "is given the same opportunity to inquire into the accuracy of the computer system involved in producing such evidence."[73]

2. If the defense is provided with a copy of the proprietary software and all evidentiary images, an expert retained by the defense will require substantial time to learn the software and recreate the process, resulting in substantial cost to the government in cases involving indigent defendants. The government will incur even further costs if the purchase of supporting operating systems and file servers is required to support the custom software.

3. While, as noted above, the source code for commercially available software is not required to be introduced into evidence in order to establish the authenticity of computer processed evidence, it is apparent that such presumptions of authenticity would not be afforded to customized software. Thus, the defense would seek to exclude the results of any computer investigation utilizing custom software tools, unless the source code was made available to the defense for testing and analysis. This would be especially true for computer forensic software, given the sensitive nature of presenting evidence of deleted files and other transient electronic information.

Conversely, when questioned in court regarding the reliability of a commercially available software application such as EnCase, the proponent of the evidence would be able to testify that EnCase is a widely used and commercially available software program and thus any member of the public can purchase, use and test the program. The defense could not claim prejudice by the use of EnCase as any reasonably skilled computer examiner would be able to examine the discovery copy of the evidence, nor would the government be subject to questions regarding its access to the source code of the program.

3

Expert Witness Testimony

§ 3.0 Overview

Are computer forensic investigators considered experts? Many courts outside of the United States, such as in Great Britain, employ a higher (perhaps wiser) threshold as to who is qualified to provide expert testimony on a technical subject. This chapter will discuss the threshold for qualifying a computer investigator as an expert and brief some cases where the court addressed this very issue. Also presented in this chapter are two fictional transcripts of sample direct examinations. The first example is a transcript from a mock pre-trial evidentiary hearing under either Federal Rules of Evidence 104, 702 and/or *Daubert v. Merrell Dow Pharmaceuticals*. A court may schedule such an evidentiary hearing to consider any foundational questions regarding the EnCase process. The second example is a direct examination in the context of a jury trial presenting evidence obtained from a computer forensic examination.

Although these examples are fictional, they are based upon actual investigation procedures and techniques taught in Guidance Software's training program and employed daily in the field by hundreds of agencies and organizations. These examples are by no means mandatory scripts to be strictly followed, but should provide a general reference for prosecutors in preparing direct examinations of their computer examiners in the context of either an evidentiary hearing or a jury trial.

§ 3.1 Threshold Under Rule 702

In the United States, *Federal Rule of Evidence* 702 provides that in order for a witness to be qualified as an expert, the expert must simply be shown to have "knowledge, skill, experience, training, or education" regarding the subject matter involved. Under this threshold, trained computer forensic experts have qualified as experts in the US courts. However, oftentimes prosecutors opt not to offer the examiner as an expert, especially where the records in question can be authenticated under *Federal Rule of Evidence* 901(b)(9) or a corresponding state statute, or where the examiner can be offered as a percipient witness presenting more objective and empirical findings of their investigation. This approach tends to be more common in many state courts.

This question was directly addressed in the recent case of *United States v. Scott-Emuakpor,*[74] where the court considered whether the United States Secret Service agents who conducted the computer forensic examination needed to be a qualified expert in computer science to present their findings.

The Defendant in *Scott-Emuakpor* brought a motion *in limine* contending that the USSS agents should be precluded from providing testimony regarding the results of their computer examinations, particularly as one of the agents admitted that he was not an expert in the area of computer science. However, the court opined that:

> "[T]here is no reason why either witness may not testify about what they did in examining the computer equipment and the results of their examinations. The question before the Court at this time is not whether these witnesses have the expertise, for example, to develop sophisticated software programs. The question is whether they have the skill to find out what is on a hard drive or a zip drive. Apparently, they have this skill because they determined what was on the drives. By analogy, a person need not be an expert on English literature in order to know how to read. . . .The fact that (the USSS agent) admitted that he is not an expert in the area of computer science is not binding on the Court."

However, it is not uncommon for an examiner to be asked to interpret the recovered data. The recent case of *United States v. Hilton*[75] provides a very good example of a computer forensic examiner offering expert witness testimony to interpret the data gleaned from his examination. Among the issues in Hilton was whether the Defendant had utilized interstate commerce (i.e. the Internet) in the process of distributing child pornography, thereby satisfying a key element and requirement of the statute. The computer investigator from the United States Customs Service testified that the images in question were located in a subdirectory named "MIRC," which contained software and files related to "IRC" (Internet Relay Chat). The Special Agent testified that, in his expert opinion, because the contraband was located in the MIRC subdirectory that contained Internet chat-related files, the images were likely associated with the Internet.

The special agent also testified that the file time and date stamps reflecting the creation time of each of the subject images were indicative that the Defendant downloaded the images from the Internet via a modem. The special agent based this conclusion on the fact that the images were created on Defendant's computer at intervals of time consistent with downloading the images via a modem. The special agent's expert testimony, among other factors, convinced the court the subject images were transmitted to the Defendant's computer via the Internet, thereby satisfying the interstate commerce requirement of section 18 U.S.C. § 2252A(a)(5)(B).

§ 3.2 Illustrations of Testimony

DIRECT EXAMINATION -- PRE-TRIAL EVIDENTIARY HEARING

A. PREFACE

If any challenge is raised to the qualifications of the computer examiner or the foundation of the evidence concerning the tools or methodologies used in the course of a computer forensic investigation, many prosecutors prefer to address such objections outside the presence of the jury through a hearing under either Federal Rule of Evidence 702, Rule 104 or *Daubert*. Judges are typically more receptive toward technical evidence and it is obviously desirable to avoid presenting complex testimony on contested technical issues before a jury by resolving such foundational issues in a separate hearing beforehand. The following fictional "mock trial" direct examination is designed to illustrate how a proper foundation may (but certainly not must) be established for the EnCase process under both Rule 901(b)(9) and *Daubert*. For illustration purposes, the below example contains more detail than what would normally be presented on direct examination, even in the context of a court trial or hearing. However, much of the information may be useful for re-direct examination.

B. BACKGROUND

[After stating name for the record]

Q: Sir, are you a Senior Special Agent for the United States Customs Service?
A: Yes I am.
Q: And do you have any specialized duties as a Customs agent?
A: I am a computer evidence examiner certified as a Seized Computer Evidence Recovery Specialist by the United States Department of the Treasury.
Q: Please tell us how long you have been a computer evidence examiner.
A: I have been a Seized Computer Evidence Recovery Specialist with Customs for eight years.
Q: Tell us about your educational background.
A: I received a Bachelor of Science degree in electrical engineering from University of _____ in 19__.
Q: And could you briefly describe your training for the handling and examination of computer evidence?
A: In 19__ I received three-weeks of intensive training, known as Seized Computer Evidence Recovery Specialist training at the Federal Law Enforcement Training Center. In 19__ I obtained Computer Forensic Examiner Certification from the International Association of Computer Specialists, known as IACIS, after receiving two weeks of their intensive training. The next year I received Advanced Course

Certification from IACIS after taking their two-week advanced training course. I have also received computer forensic training from The National Consortium for Justice Information and Statistics, known as SEARCH and have received training from Guidance Software on their EnCase computer forensic application.
Q: Are you a member of any professional organizations?
A: Yes I am.
Q: Which ones?
A: I am a member of the International Association of Computer Specialists, and the High Tech Crime Investigation Association.

C. OVERVIEW OF COMPUTER FORENSICS

Q: You mentioned the subject of computer forensics. Can you provide an overview of what computer forensics is?
A: Computer Forensics is the acquisition, authentication and reconstruction of electronic information stored on computer media, such as hard drives, floppy disks or zip drives. A computer forensics technician is needed whenever there is evidence stored in a computer.
Q: Can you briefly tell us how a computer forensic specialist such as yourself conducts a typical investigation?
A: First, the electronic information contained on computer storage media must be acquired by making a complete physical copy of every bit of data located on computer media in a manner that does not alter that information in any way. Then the information must be authenticated in a special process that establishes that the acquired electronic information remained completely unaltered from the time the examiner acquired it. Finally, the examiner must use special software and processes to recover and reconstruct the information in its forensic state, even if such information is found in files that have been deleted by the user.

D. THE ACQUISITION PROCESS

Q: You described three basic steps, and I want to discuss them one at a time beginning with the acquisition process. How is digital information copied from computer media in a proper forensic manner?
A: Specialized computer forensic software, such as EnCase, utilizes a special boot process that ensures the data on the subject computer is not changed. After the boot procedure is initiated, the examiner utilizes the forensic software to create a complete forensic image copy or "exact snapshot" of a targeted piece of computer media, such as a hard drive, or external media, such as floppy or zip disks. This forensic image is a complete sector-by-sector copy of all data contained on the target media and thus all information, including available information from deleted files, is included in the forensic image created by the

examiner.

E. THE AUTHENTICATION PROCESS

Q: The second step you mentioned was the authentication process; please briefly describe how the acquired electronic information is authenticated and verified.
A: Computer forensic examiners rely upon software that generates a mathematical value based upon the exact content of the information contained in the forensic image copy of the seized computer media. This value is known as an MD5 hash value and is often referred to as a special type of digital signature. The same software also verifies that this value remains the same from the time it is generated. If one bit of data on the forensic image copy is subsequently altered in any way, meaning that even if a single character is changed or one space of text is added, this value changes. So if the hash value of the information contained on seized media remains the same, then it is established that the electronic data has not been altered in any way.
Q: What are the odds of two forensic images with different contents having the same hash value?
A: The odds of two computer files, including a forensic image file, with different contents having the same hash value is roughly ten raised to the 38^{th} power. If you wrote out that number, it would be a one followed by 38 zeros. By contrast, the number one trillion written out is one followed by only twelve zeros.

F. THE RECOVERY PROCESS

Q: Because the third step of data recovery is complex, I am going to first ask you a few basic questions about how a computer works. First, and without being too technical, could you give us a description of how information on a hard drive is stored by the computer?
A: Yes. Basically, computer disks are storage media that are divided into concentric circles or tracks. This can be thought of as a small version of the old 78 rpm records people used to play on phonographs. The tracks are divided into sectors. Each sector has its own address, a number that is unique to that part of the disk. The operating system assigns and stores the address, so that it may retrieve all information constituting a computer file stored in a specific sector when requested by the user.
Q: How is the information recorded on the hard disk?
A: The disk is covered with a thin coat of magnetic material. When information is written to the disk, the data is recorded by magnetizing specific parts of the disk coating. The information resides there until it is overwritten.
Q: Thank you. I think we have the basic idea. I am very interested in

how a computer technician can recover electronic information that has been deleted or automatically purged. Please tell us what is involved in this process.
A: When the computer user deletes electronic information, it is often assumed that the information is removed from the computer forever. That is not necessarily true. The information is still in the computer; only it is now marked by the computer to allow it to be overwritten. A general analogy would be a library card catalogue system, where the books represents files and the card catalogue represents the file directory with information as to where the files are located on the disk. When a file is deleted, its location information is removed from the card catalogue index, but the book remains on the shelf until another book randomly replaces it.
Q: To what extent can this deleted information be retrieved?
A: If the information has not yet been overwritten by other data, it is still there and can be retrieved using specialized software.

G. AUTHENTICATING THE ENCASE PROCESS UNDER RULE 901

Q: And what specialized software did you use for this investigation?
A: I used the computer forensic software known as EnCase.
Q: Tell us a little about the EnCase software.
A: EnCase is a standard, commercially available software program that is specifically designed as a tool for computer forensic investigations. It is a fully integrated tool, meaning it performs all essential functions of a computer forensic investigation, including the imaging of a target drive, the generation of an MD5 hash of the evidentiary forensic image, and the analysis of the subject evidence. The software allows for a completely non-invasive investigation in order to view all information on a computer drive, whether it is in the form of a deleted file, a non-deleted file, file fragments and even temporary or buffer files.
Q: How does the investigator use the EnCase software to recover deleted files?
A: First, EnCase creates a complete forensic image copy or "exact snapshot" of a targeted computer drive. EnCase will be able to read all existing information on that forensic image, regardless of whether the information is in the form of a deleted file that is marked by the operating system to be overwritten. Any information that has not been actually overwritten will be recovered for analysis. EnCase will organize all the files, deleted files and blocks of physical data, also known as unallocated clusters, in a convenient graphical user interface to allow the evidence to be viewed and sorted by the examiner.
Q: Does the same software perform these functions?
A: Yes. EnCase is a software process that is much more automated

than other computer forensic investigation processes, as it is a fully integrated program where all the required computer forensic investigation functions are integrated into a single application in a Windows-based graphical user interface.
Q: How is the EnCase process more automated than other tools?
A: To a large extent EnCase duplicates the Windows Explorer interface and file viewing functions, with the critical added benefits of viewing deleted files and all other information on the disk that the user normally cannot see or detect without specialized software. Just as Windows Explorer presents the entire file directory and folder structure on a computer to the user in a very organized manner, EnCase will also present that information, in addition other data on the target drive in a similar manner. Other forensic software tools require a great deal of more manual steps utilizing a series of arcane DOS commands and separate tools to recreate file structures and perform separate searches on different areas of a drive.

H. ADDRESSING *DAUBERT* FACTORS

Q: To your knowledge, is the EnCase software generally accepted in the computer forensic investigation community?
A: More than just generally accepted, EnCase is widely used in the computer forensics industry, and in my experience it is the tool of choice of the majority of computer forensic investigators in law enforcement. It is the primary computer forensic tool used by US Customs, which is my agency, and I am aware that it is the primary tool of other federal agencies, including United States Secret Service, as well as hundreds of state and local agencies. EnCase is a major part of the Seized Computer Evidence Recovery Specialist training curriculum for federal agents, and is part of the curriculum in many computer forensic training courses offered by professional organizations — most notably the annual IACIS training conference.
Q: How would one go about testing computer forensic software?
A: There are three main steps in testing computer forensic software. The first step is to generate an MD5 hash value for an image of a targeted computer drive using the forensic tool being tested and then using another standard tool to repeat the process for the same drive. The MD5 hash values generated by both tools for the same drive should be exactly the same. The second step is to verify that whatever evidence is recovered from an evidentiary forensic image can be independently confirmed by a standard disk utility. With EnCase for instance, the program will identify the precise location on the original drive for each bit of data recovered by the examiner. With that information, the examiner can then use a disk utility such as Norton DiskEdit to independently confirm the existence and precise location of that data. The third step is to confirm that throughout the examination process, the content on the forensic image has not been

altered in any way by repeating the MD5 hash analysis of the forensic image to verify that the MD5 hash is has not changed since the time of acquisition. These tests should be performed several times with different pieces of computer media.
Q: To what extent can EnCase be tested by a third party?
A: EnCase is commercially available and thus any examiner can purchase, use and test the program on their own. One of the advantages of the program is that all the required forensic functions are integrated into a single program with a Windows-based graphical user interface. Thus, compared to other computer forensic software, the program is easy to use.
Q: Has your agency tested the software?
A: Yes.
Q: How was it tested?
A: Before we purchased the software on a large scale, there were two computer investigation agents in my agency who conducted an extensive evaluation of the software employing the three steps I just described. I am aware that the Secret Service conducted a similar testing procedure as well. Also, since our agencies' adoption of the software we have had nearly 100 computer examination agents using the program on a daily basis in the field.
Q: What were the results of those tests?
A: By all accounts the software has met the three standards I described above.
Q: Has EnCase been subjected to any publication in the industry that you are aware of?
A: Yes, I have read various published articles in the information security and high-tech crime investigation industries that either favorably review the product or mention the product favorably. A recent article in the April 2001 issue of SC Magazine featured the most detailed and documented published testing results to date. The magazine gave EnCase its highest rating and noted that in its testing EnCase "outperformed all the other tools" that were tested by the magazine.
Q: At this time Your Honor, I'd like to submit as the Government's exhibit __, which are copies of published articles in the industry discussing the EnCase software.[76]
THE COURT: So received.
Q: Thank you, Your Honor, nothing further.

DIRECT EXAMINATION FOR THE PRESENTATION OF COMPUTER EVIDENCE BEFORE A JURY

A. PREFACE

Many prosecutors maintain that when presenting computer evidence before a

jury, the testimony should be as simple and straightforward as possible. Burdening the jury with overly technical information could prove counter-productive and may actually open the door to areas of cross-examination that the court would normally have disallowed. As such, the following direct examination is more detailed than is likely needed, but again, should provide a general resource in preparing direct examinations or for responding on re-direct. Further, there are many other foundational areas that are normally outside the scope of the EnCase process, such as establishing how an Internet chat room works, what the Windows operating system is, or establishing that the computer belonged to the defendant, which are not addressed here. (For a good discussion of establishing a foundation for a printout of a chat room conversation, see *United States v. Tank.*[77])

When presenting EnCase-based evidence, it is recommended that the proponent take full advantage of the EnCase process and graphical user interface by presenting screen shots of the EnCase "All Files" and other views, in order to show the full context of the electronic evidence. This technique may also be required to comply with Best Evidence Rule considerations in computer evidence. Federal Rule of Evidence 1001(3) provides "[if] data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'" When presenting evidence contained within a computer file, a screen shot of the EnCase File View may be the best means to present a visual output which is "shown to reflect the data accurately," and thus constitute an "original" under Rule 1001(3). (See Chapter 4 for a more detailed discussion of the Best Evidence Rule.)

When seeking to establish a defendant's state of mind by presenting an electronic audit trail or connecting file date stamps, the ability to display a visual output showing various file attributes and other metadata provides a tremendous advantage to the advocate of such evidence. EnCase provides the best method to visually display all physical and logical data contained on the target drive, while showing the context of such files by displaying file metadata and other means. When providing testimony, many examiners present evidence through screenshots in a PowerPoint presentations format, or take EnCase with them into Court for a more live demonstration. In *United States v. Dean*, (discussed further in § 4.2) the opinion reflects that the prosecution presented results of its computer forensic examination through PowerPoint.[78]

Please note that for sake of brevity, many of the foundational portions of the direct exam are incorporated by reference from the above section.

[After stating name for the record]

B. BACKGROUND

Q: Sir, what is your current occupation?
A: I am a Senior Special Agent for the United States Customs Service.
Q: And do you have any specialized duties as a Customs agent?
A: I am a computer evidence examiner certified as a Seized Computer

Evidence Recovery Specialist by the United States Department of the Treasury.
Q: What was your involvement in the investigation of this case?
A: I conducted a computer forensic investigation of the Defendant's computer to recover relevant evidence.
Q: OK, before we discuss the results of your investigation, please tell us how long you been a computer evidence examiner.

[Please Refer To Previous Section, which is incorporated herein by reference, for foundation testimony]

* * * *

Q: Turning to the computer forensic investigation you conducted in this case, please tell us when you first came into contact with the Defendant's computer and computer disks.
A: Pursuant to a search warrant, on May 18, 2000 I seized the Defendants computer at his home, along with seven CD-ROMs and sixteen floppy disks that were in his desk or otherwise in the vicinity of his computer.
Q: What did you do with the Defendants' computer equipment and disks after you seized them?
A: After leaving receipts for the computer and disks, I transported the items back to our lab, where I immediately proceeded to make forensic image copies of the hard drive found in the Defendant's computer. I also made forensic images of each of the CD-ROM and floppy disks. Using the EnCase software, I also generated MD5 hash values for the hard drive and for each floppy and CD-ROM disk at the same time the forensic images were made. I then logged the Defendant's computer and the floppy and CD-ROM disks as evidence and secured them into our evidence storage room.
Q: Did you then analyze the forensic images you made?
A: Yes I did.
Q: Please describe your analysis on the forensic image of the Defendants' hard drive.

C. RECOVERY OF HIDDEN FILES WITH RENAMED FILE EXTENSIONS

A: In my analysis of the forensic image of the hard drive, I first employed an automated function of the EnCase forensic software that analyzes all the computer files on an image of a computer drive and identifies any file signature mismatches.
Q: What are file signature mismatches?
A: A file signature mismatch is a situation where the file name extension that normally identifies the file type has been renamed, usually in order to hide the true contents of a file.

Q: What is a file name extension?
A: A file name extension is an optional addition to the file name that allows a file's format to be described as part of its name so that users can quickly understand the type of file it is without having to open files on a trial and error basis. For instance, a text file will usually have a ".txt" extension and the most common type of picture file has a ".jpg" extension.
Q: How does EnCase identify file signature mismatches?
A: Most computer files containing text or graphical images have a well-defined signature of electronic data unique to that file type. This allows file viewers to recognize the type of file, regardless of the file extension. EnCase utilizes the same process as file viewers in order to identify files that have renamed file extensions.
A: What was the result of the file mismatch analysis that you conducted in this case?
Q: The file signature mismatch analysis revealed 16 files that were renamed as text files with a "txt" extension, but were actually graphical image files that originally had a "jpg" extension until they were renamed manually. I viewed those files and upon determining that those images appeared to be child pornography, I printed out those images.
Q: Showing to you what have been pre-marked as United States exhibits 1 through 16, can you identify these exhibits?
A: Yes. These are the printouts I made of the 16 images in question that I recovered from the Defendant's hard drive.
[Exhibits are introduced into evidence.]

D. RECOVERY OF DELETED FILES

Q: Did you examine the images you made of the Defendant's floppy disks?
A: Yes I did.
Q: What did you find?
A: I found that one of the floppy disks had five files with a "jpg" extension that had been deleted, meaning that that the computer had marked the data of those files to be overwritten. However, we were able to still recover those deleted graphical image files as the data had not actually been overwritten by the computer.
Q: How did you identify those deleted files?
Q: The EnCase software will automatically identify any files that are marked by the computer to be overwritten. I located and viewed those five graphical image files and upon determining that those images appeared to be child pornography, I printed out those images.
Q: Showing to you what have been pre-marked as United States exhibits 17 through 22, can you identify these exhibits?
A: Yes. These are the printouts I made of the five images that I

recovered from the Defendant's reformatted floppy drive.
[Exhibits are introduced into evidence.]

E. RECOVERY OF FILES "DELETED" FROM MULITPLE CD-ROM SESSIONS

Q: Special Agent _____, did you examine the images you made of the Defendant's CD-ROM disks?
A: Yes I did.
Q: And what did you find?
A: I found that the CD-ROM disks were actually writeable, meaning that data can be written to this type of compact disk to store computer files. A special CD writing software program, such as CD Creator, is needed to write data to a writeable compact disk. One of the writeable CDs we seized from Defendant's home had multiple sessions on it. A CD session is created when the user writes any number of files to the CD. When this is done, the CD writing software will create a table of contents for that session that points the operating system to the location of the files on the CD within the session.
Q: Can files on a writeable CD be deleted?
A: Not really. Unlike a hard drive or floppy disk, data written to a CD is actually burned to the media by a small optical laser instead of being magnetized. Once data is burned to a CD, it cannot be overwritten. However, if a new session is created on the CD, the user can omit existing files from the new table of contents created for the new session. A computer operating system will only read the table of contents from the latest created session on a CD. Thus, by omitting existing files from the table of contents of a new session, those files will normally be hidden from the view of a user. Specialized software, such an EnCase, will see all the sessions on a writeable compact disk and will allow the user to compare any differences in the file contents of each session.
Q: You mentioned that one of the CDs you examined had multiple sessions. What did your analysis of the multiple session CD reveal?
A: The CD actually had two sessions on it. Using EnCase, we discovered that the second session contained seven files with jpg extensions that were not included in the table of contents of the first session. I then examined those seven files, which turned out to be graphical images appearing to be child pornography, and printed out those images.
Q: Showing to you what have been pre-marked as United States exhibits 23 through 30, can you identify these exhibits?
A: Yes. These are the printouts I made of the seven images that I recovered from the first session of Defendant's writeable compact disk.
[Exhibits are introduced into evidence.]

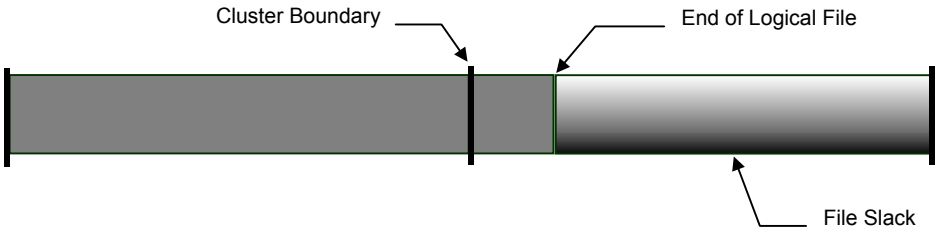
F. EVIDENCE FROM SWAP FILES

Q: What else did you find in your examination of the Defendant's computer?
A: I conducted a text string search of the forensic image of the Defendants hard drive. In the course of our investigation, we received information that the defendant had contacted a minor over the Internet who had an America Online account under the screen name Jenny86. I ran a text search by entering the keyword Jenny86, again using the EnCase software. The search registered several hits in an area of unallocated clusters identified by EnCase as a swap file.
Q: What is a swap file?
A: A swap file is a random area on a hard disk used by the computer's operating system to temporarily store data as a means to manage the available operating memory of a computer. The operating system will swap information as needed between the memory chips and the hard disk in order to process that information. As a result, temporary data is placed on the computer that cannot be viewed without special software designed for that purpose.
Q: What type of data is typically written to the swap file?
A: Any data that appears on the computer screen, even in the form of an unsaved word processing document or a Web page being viewed by the user, is often written to the swap file by the operating system.
Q: What did you do after you identified search hits for the keyword Jenny86 in the swap file area?
A: I retrieved the full text of the information contained in the swap file and printed it out.
Q: I'm now handing you what has been previously marked as exhibit 31, and ask if you can identify it?
A: Yes. This is the print-out I made of the data contained in the swap file where my keyword search registered hits for the keyword Jenny86.
Q: If you would, please read the text as it appears on this printout.
A: The text appears in transcript form and reads, "Welcome to Yahoo Young Teen Chat …. [full text is read]"
[Exhibit is introduced into evidence.]

G. EVIDENCE FOUND IN FILE SLACK

Q: What else did you find in your examination of the Defendant's computer?
A: I conducted a separate text string search of the forensic image of the Defendant's hard drive. In our investigation, we received additional information that the Defendant had corresponded approximately one to two years ago to another individual on more than one occasion. That person has since been convicted of possession of

child pornography and sexual assault on a minor. This person's name is John Doe, and he commonly went by the nickname Lolita's Man. We conducted a text string search with the keyword Lolita's Man and registered a hit in an area of data known as file slack, which contained remnants of a deleted file.
Q: What is file slack?
A: Data storage areas on a hard disk are segmented into clusters. All the data constituting a file may occupy an entire cluster, or the file data may not take up all of the space in the physical cluster. The space between the end of a file and the physical end of a cluster is called the file slack. After the point in the cluster where the file ends, there may be pre-existing bytes in a cluster that are remnants of previous files or folders. *[NOTE: A projected PowerPoint slide or other form of demonstrative graphic illustrating this issue would be effective at this part of the examination.]*



Example of A Demonstrative Trial Graphic

Q: What did you do after you identified search hits for the keyword John Doe in the area of file slack?
A: I retrieved the full text of the remainder of the document contained in the file slack, and printed it out.
Q: Could you determine what kind of document the remnant text in file slack was a part of?
A: Based upon my observation of the format of the two remaining paragraphs in the document and the signature block at the end of the document, it appears that the text recovered from file slack was the remnants of a correspondence of some type.
Q: I'm now handing you what has been previously marked as exhibit 32, and ask if you can identify it?
A: Yes. This is the print-out I made of the data contained in the file slack area where my text search registered a hit for the text string search Lolita's Man.
Q: If you would, please read the text as it appears on this print-out.
A: [The text is read into the record]
[NOTE: Because oral testimony of the recovery of file slack may seem too abstract to the jury and the court and because of best evidence rule considerations, it is recommended that a full screen shot of EnCase in

from the "File View" with the highlighted text hit in file slack be projected in order to show the full context of the relevant text].
Q: Showing what has been pre-marked as exhibit 33 on the projection screen, does this look familiar to you?
A: Yes, that is a screen shot of the File View of EnCase I created, showing the search hit for "Lolita's Man" in file slack.
Q: Part of the text on the screen is in red, while the text before it is in normal black font. Does the text coloring have any significance?
A: The black text is the active, or non-deleted file that occupies the point from the beginning of the cluster to the end of that file. The red text represents the file slack in the area from the end of the non-deleted file to the end of the cluster.
[Exhibits 32 and 33 are introduced into evidence.]

H. EVIDENCE OF WINDOWS METAFILES RECOVERED FROM UNALLOCATED CLUSTERS

Q: What else did you find in your examination of the Defendant's computer?
A: As part of my routine practice, I recovered all Windows metafiles that were located on the hard drive.
Q: What are Windows metafiles?
A: When a user sends a command to print a file, the Windows operating system makes a copy of that file and sends the copy to the printer. After the file is sent to the printer, Windows deletes that file. Windows does not inform the user that the copy, or metafile, has been made, nor can the user usually detect the existence of the metafiles without special software.
Q: How did you recover the metafiles in this case?
A: The EnCase software has an automated function that locates all the metafiles residing in normally unseen areas on a hard drive, decodes them, and outputs them to a separate folder allowing them to be viewed.
Q: What did you do after you utilized this software function that located the metafiles and outputted them to a folder?
A: I opened the folder and viewed each of the recovered metafiles.
Q: What did you find?
A: I found a text document in an e-mail format addressed to the Defendant's e-mail account. According to the e-mail header information, the message was sent from the account of Jenny86@hotmail.com.
Q: What does the fact that this e-mail document existed in the form of a metafile mean to you?
A: This recovered metafile means that this e-mail message was printed out from the Defendant's computer.
Q: I'm now handing you what has been previously marked as exhibit

34, and ask if you can identify it?
A: Yes. This is the printout I made of the metafile of the e-mail document from Jenny86@hotmail.com to the e-mail account of the Defendant.
Q: If you would, please read the text as it appears on this printout.

4

The Best Evidence Rule

§ 4.0 Overview

Probably the most misunderstood rule of evidence among many computer forensic investigators is the Best Evidence Rule. The Best Evidence Rule is a doctrine of evidentiary law in the United States and Canada that essentially requires that, absent some exceptions, the original of a writing must be admitted in order to prove its contents. As one might imagine, significant questions arise when applying this evidentiary doctrine to computer data. Among the issues raised by this rule are how to present computer evidence at trial, what constitutes a valid image of a computer drive, and data compression. This chapter will provide the law and address some myths as well.

§ 4.1 "Original" Electronic Evidence

The Best Evidence Rule under the US Federal Rules provides that "[t]o prove the content of a writing, recording or photograph, the original writing, recording or photograph is required…"[79] Notably, electronic evidence falls under the Federal Rules definition of "documents." [80] However, with electronic evidence, the concept of an "original" is difficult to define. For example, when seeking to reproduce an original photographic image, a negative of that photograph, while containing all the "data" of the original, must be processed in order to provide an accurate visual replication of the original photograph. Fortunately, the Federal Rules of Evidence have expressly addressed this concern. Rule 1001(3) provides "[if] data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'" Under this rule and similar rules in state jurisdictions, multiple or even an infinite number of copies of electronic files may each constitute an "original."[81]

The operative language in Rule 1001(3) is "accurate reflection." It is a mistake to analogize computer files to hard copy documents for purposes of the Best Evidence Rule. A mere bit stream copy of a graphical image file does not provide a completely accurate "printout or other output readable by sight" unless Windows-supported forensic tools or other viewers are used to non-invasively create an accurate visual output of the recovered data, without changing any of the data. Conversely, if a computer file is compressed, encrypted, transmitted as an e-mail attachment (thus sending a copy of that decrypted, compressed file in a different file format and even divided into many packets), and then received, decompressed, decrypted and opened, the file now in possession of the recipient would be another 'original' of that file under the Federal Rules. Printing that file also converts it to another file format. However, as long as the printout is an accurate reflection of the original data, it is irrelevant what the operating system or the network

does to that file during the printing process.

The important concept here is the accuracy of the visual output once the image is mounted. If an examiner were to simply extract key data from slack space and export that data to a text file, will a printout of that text file always constitute an accurate reflection of the original data? Many prosecutors do not think so, because the context of computer data is often as important as the data itself. Congress, by enacting Rule 1001(3), placed the emphasis on the accuracy of the visual output of computer data (printout or otherwise) once the image or file is mounted, not on the stored state of that file or image. Obviously, if the original data is actually compromised, the visual output will not be accurate. It is mandatory that the original data remain unchanged, but whether that data is compressed, encrypted or converted to a different file format in its stored state is immaterial as long as the data itself is not compromised. This is one of the reasons the MD5 hash and verification processes are so important. Even though the file format of the data in question may change, the integrity of that data must remain intact.

The Best Evidence Rule has been raised in the context of an entire drive image as well as an individual file. A Texas Appellate Court recently ruled that an image copy of a hard drive qualifies as an "original" for the purposes of the Best Evidence Rule.[82] The issue of whether an EnCase Evidence File suffices as an "original" under the Best Evidence Rule was recently litigated successfully in US Federal District Court, New Hampshire (see § 4.4 for a full discussion).

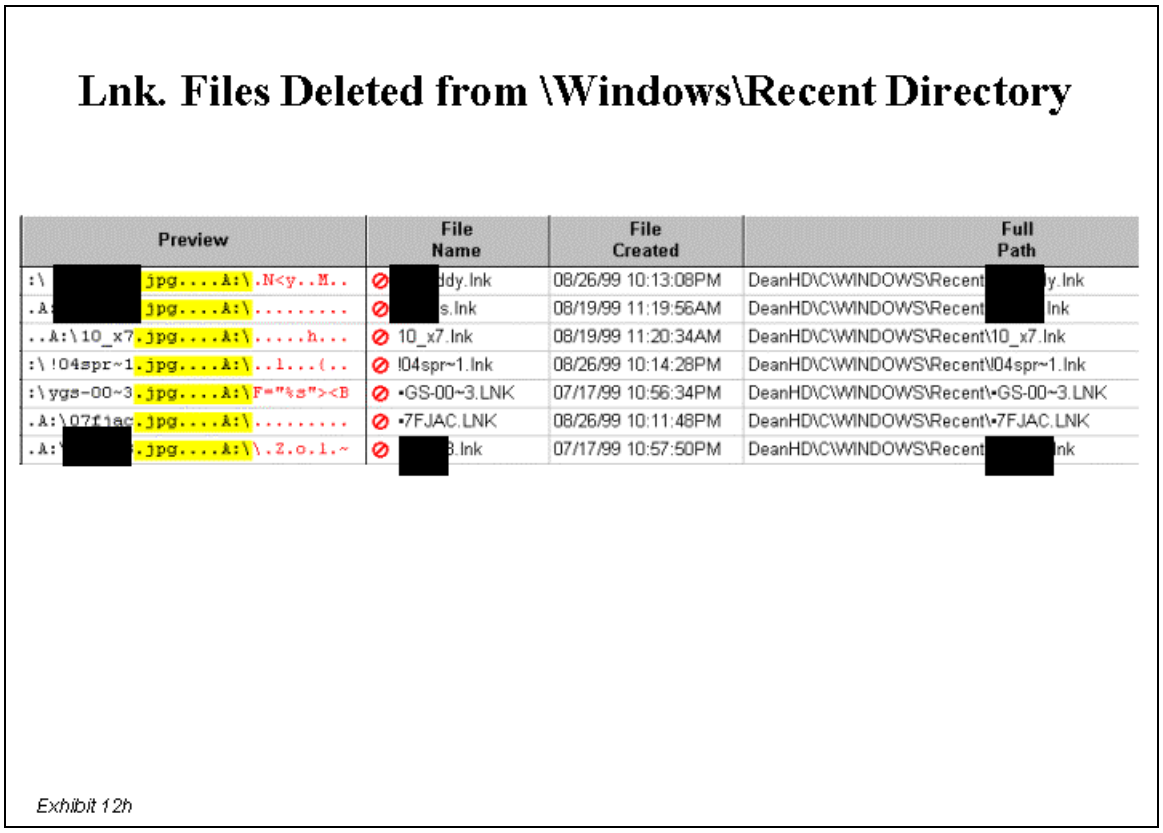
In situations where computer evidence is collected from a business, a drive image copy is often the only "original" available to the examiner, as the company often requires immediate return of the original drives in order to remain in business. However, while there is strong legal support for a drive image copy satisfying the Best Evidence rule, it is always advisable to retain physical custody of the seized drive whenever possible. An ideal compromise is to retain custody of the original drives while providing restored or cloned drives to the business.

§ 4.2 Presenting Electronic Evidence at Trial

The United States DOJ Guidelines on Searching and Seizing Computers states "an accurate printout of computer data always satisfies the best evidence rule."[83] This certainly is true in general. However, in *Armstrong v. Executive Office of The President,*[84] the court correctly ruled that a "hard copy" paper printout of an electronic document would not "necessarily include all the information held in the computer memory as part of the electronic document."[85] The court further noted that without the retention of a complete digital copy of an electronic document such as an e-mail message, "essential transmittal relevant to a fuller understanding of the ***context and import*** of an electronic communication will simply vanish."[86]

As illustrated by the *Armstrong* case, the presentation of electronic evidence often requires the visual display of the logical data structure of a file, its context, and its associated metadata, in addition to the physical data of that file. When seeking to

establish a defendant's state of mind by presenting an electronic audit trail, the ability to display a visual output showing various file attributes and other metadata and demonstrating the logical connection to various data files—instead of relying upon dry and technical expert testimony—provides a tremendous advantage to the advocate of such evidence. EnCase provides the best method to visually display all physical and logical data contained on the target drive, while showing the context of such files by displaying file metadata and other means. When providing testimony, many examiners present evidence through screenshots in a PowerPoint presentations format, or take EnCase with them into Court for a live demonstration. In *United States v. Dean*, the opinion reflects that the prosecution presented results of its computer forensic examination through PowerPoint slides.[87] Such a presentation, fast becoming common if not mandatory in modern trial practice, is virtually impossible using the available command-line utilities.



Lnk. Files Deleted from \Windows\Recent Directory

Preview	File Name	File Created	Full Path
:\ [redacted] jpg....A:\.N<y..M..	[redacted]ddy.lnk	08/26/99 10:13:08PM	DeanHD\C\WINDOWS\Recent[redacted]y.lnk
.A:[redacted] jpg....A:\.....	[redacted]s.lnk	08/19/99 11:19:56AM	DeanHD\C\WINDOWS\Recent[redacted]lnk
..A:\10_x7.jpg....A:\.....h...	10_x7.lnk	08/19/99 11:20:34AM	DeanHD\C\WINDOWS\Recent\10_x7.lnk
:\!04spr~1.jpg....A:\..l...(..	!04spr~1.lnk	08/26/99 10:14:28PM	DeanHD\C\WINDOWS\Recent\!04spr~1.lnk
:\ygs-00~3.jpg....A:\F="%s"><B	•GS-00~3.LNK	07/17/99 10:56:34PM	DeanHD\C\WINDOWS\Recent\•GS-00~3.LNK
.A:\07f1ac.jpg....A:\.....	•7FJAC.LNK	08/26/99 10:11:48PM	DeanHD\C\WINDOWS\Recent\•7FJAC.LNK
.A:[redacted].jpg....A:\\.Z.o.l.~	[redacted]3.lnk	07/17/99 10:57:50PM	DeanHD\C\WINDOWS\Recent[redacted]nk

Exhibit 12h

Figure 1: A screenshot exhibit offered by the prosecution and entered into evidence in *US v. Dean*. The black redactions over certain filenames are a result of the *Dean* court's ruling that the probative value of those filenames was outwieghed by their prejudicial nature.

In *Dean*, the prosecution sought to establish that the Defendant accessed and viewed files on a series of floppy disks. While the Defendant denied ever accessing and viewing those files, his computer operating system created temporary link files when he accessed the floppy disk files. A US Customs Service forensic investigator recovered those temporary link files from the Defendant's hard drive. In order to show the context

and metadata associated with the link files, including file created dates, full path location and other information, the prosecution successfully presented EnCase screen shots as evidentiary exhibits. These screen capture exhibits provided the most accurate visual display of the data, as it existed on the Defendant's computer at the time of seizure. The court allowed the screenshots into evidence and Dean was convicted on all counts.

Dean is an important illustration that the context of computer evidence is often just as important as the data itself. For example, if portions of relevant data are recovered in unallocated or slack space areas of a drive and then simply exported to a text file and then printed, a proponent will likely face significant difficulty in admitting that evidence without establishing its context. What file partially overwrote the first section of the cluster where the slack data still resides? When was the file currently occupying that cluster created and last modified? What is the precise address (physical cluster, sector offset, etc.) of the data recovered from slack space? Figure 2 illustrates how such data should be presented both for demonstrative purposes and to comply with the Best Evidence rule.

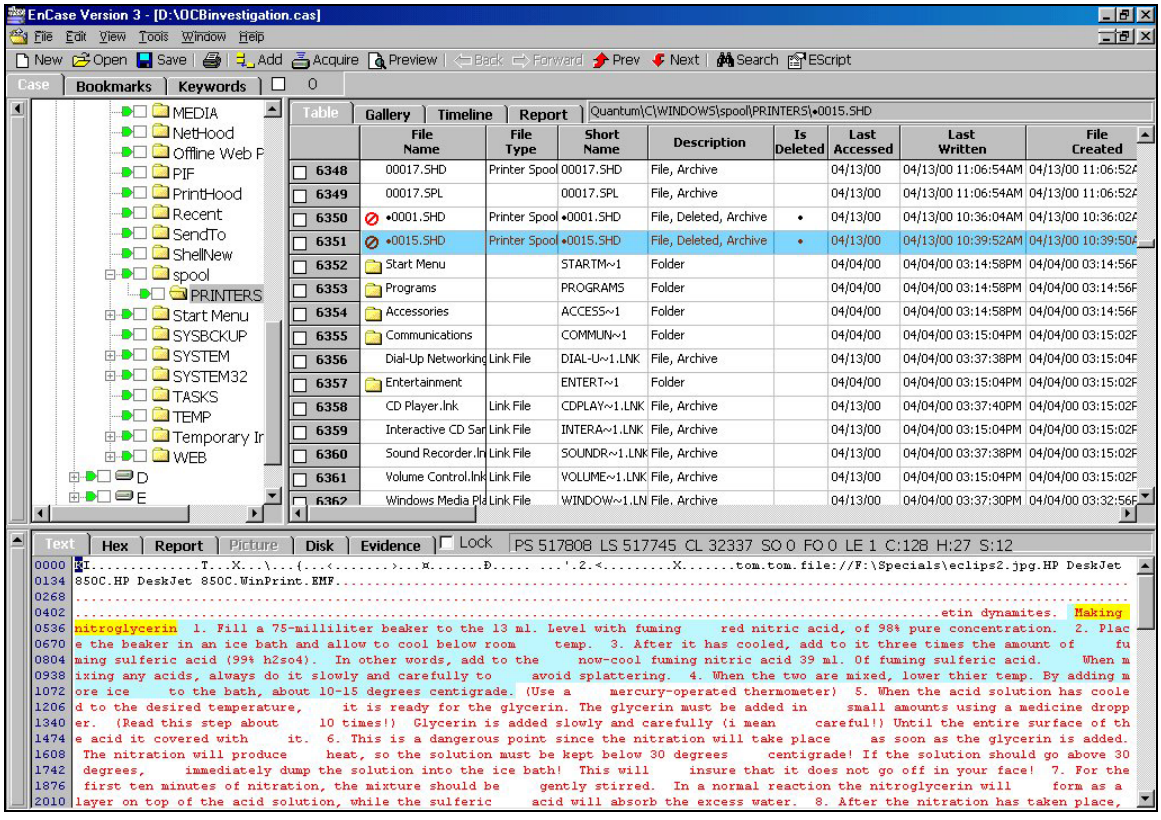


Figure 2: Key evidence of bomb making instructions found in the slack area of a cluster also occupied (at the beginning) by a deleted printer spool file. Screen shot presentation enables full contextual presentation of the data.

§ 4.3 Compression And the Best Evidence Rule

The issue of compression in the context of computer evidence is one that has

never been addressed by the courts in any known published decisions. However, there is some appreciable authority where US courts have discussed data compression in the context of intellectual property disputes. These rulings do provide a degree of guidance on how the courts would address compressed computer files as evidence.

In *Storer v. Hayes Microcomputer Products*, the court defined computer data compression as follows: "Data compression is the process of reducing the size of the representation of a string of electronic data in order to permit it to be transmitted or stored more efficiently and later to be reconstructed without error."[88] While the *Storer* case addressed whether a company's compression technology infringed upon a patent held by a competitor for similar technology, the case provides a clear and concise definition of data compression as articulated by a court. In *Universal City Studios v. Reimerdes,*[89] a Napster-genre copyright infringement case, the court determined that a software application that compresses and then decompresses DVD recordings using "lossy" compression infringes upon the copyright of the publisher. This is so even though "lossy" compression involves inexact replication of the original file. Thus, the compressed and then decompressed end product infringes upon the copyright of the original material.

Compression technology allows EnCase to store a large disk image in a relatively small file. An Evidence File can be compressed upon acquisition or at a later point in the investigation. Compressed Evidence Files can be searched and examined by EnCase in the same manner as uncompressed Evidence Files. EnCase uses an industry standard "lossless" compression algorithm to achieve an average of 50% size reduction. Lossless data compression, where the compressed-then-decompressed data is an exact replication of the original data, is a very basic and standard aspect of computer science. It is also important to note that whenever a computer file is transmitted over the Internet or it is sent to the printer, it undergoes compression. Some excellent resources on lossless data compression and data compression in general can be found at http://www.data-compression.com.

As noted above, Federal Rule of Evidence 1001(3) provides "[if] data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'" Compression does not have any effect on the actual content of the Evidence Files or the integrity of the evidence. Importantly, a compressed Evidence File will register the same CRC and MD5 hash values as an uncompressed Evidence File of the same drive, as the file content is identical. Further, in the post-acquisition verification process, EnCase verifies the compressed blocks as well as the MD5 hash for the entire image in the same manner as with uncompressed Evidence Files.

As a compressed Evidence File will contain the exact same contents and the same CRC and MD5 hash values as an uncompressed Evidence File of the same disk image, both will constitute an "original" under Fed.R.Evid. 1001(3). For the same reason, an Evidence File that is acquired uncompressed and is subsequently copied in a compressed format also constitutes an "original" under Rule 1001(3).

§ 4.4 *US v. Naparst* – The EnCase Evidence File Validated As Best Evidence

The issue of whether EnCase Evidence Files constituted the best evidence of the computer data contained therein was litigated in a recent federal criminal prosecution in New Hampshire. The prosecution offered to allow the Defense access to a copy of the EnCase evidence file for discovery purposes. However, the Defense contended that it required access to the original computer systems in question so that they could operate those computers and examine them in their native environment, and filed a formal written request for a Court order allowing such unfettered access to the "original" computer evidence. The Government filed a successful objection to the request, asserting that the "mirror image" created by the Special Agent is the proper way to preserve the original evidence, as turning on the computer, as the Defense requested, will change the state of the evidence by altering critical date stamps and potentially overwriting existing files and information.

The Court ruled that the EnCase Evidence File qualified as the Best Evidence and that a discovery copy of the Evidence File would be sufficient discovery disclosure. Alternatively, the court ruled that the defense could have access to the original computer systems only if its expert created another proper forensic image under the supervision of the Special Agent. The defense was barred from booting the original computer systems to their native operating systems. A copy of the three-page brief filed by the Government in support of its successful objection is reprinted here with permission.

UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

(United States of America
(
(v. Cr.: 00-11-1-M
(
(Harold Naparst

GOVERNMENT'S OBJECTION TO DEFENDANT'S
MOTION FOR ACCESS TO COMPUTER EVIDENCE

NOW COMES the United States of America, by Paul M. Gagnon, United States Attorney for the District of New Hampshire and states the following:

1. On August 16 & 17, 2000, an expert retained by the defense in this matter was permitted access to the government's expert witness, all of his reports, and an exact mirror image of the defendant's computer hard drives.

2. The defense has now moved this Court to grant them access to the defendant's actual computer equipment which was seized from his home on January14, 2000.

3. The defense argues that this is necessary for preparation of their defense; however, the government submits that if the defense has truly consulted with an expert, then they are aware that the mere act of turning on or "booting up" the defendant's computer will alter that evidence forever.

4. Turning on the computer will change the state of the evidence by altering critical date stamps, and will potentially write over and erase existing files. See affidavit of Shawn McCreight attached as Exhibit 1.

5. The "mirror image" created by Supervisory Special Agent Marx is the proper way to preserve the original evidence and the government will demonstrate that this evidence is the original evidence of the defendant's hard drives. See affidavits of Shawn McCreight and SSA Stephen Marx attached as exhibits 1 and 2.

6. The importance of conducting reviews of computer evidence on mirror image backups is so universally understood that in one civil action, the plaintiffs were sanctioned for failing to create a mirror image of the defendant's hard drive before their review. See Gates Rubber Company v. Bando Chemical Industries, Limited, 167 F.R.D. 90, (D. Colorado, 1996). Instead, they ran a program on the original hard drive which "obliterated, at random, 7 to 8 percent of the information which would otherwise have been available." 167 F.R.D. 90, 112. The Court, therefore ruled that sanctions were appropriate because the plaintiff "had a duty to utilize the method which would yield the most complete and accurate results" and "should have done an 'image backup' of the hard drive which would have collected every piece of information on the hard drive…"

Id.

7. Defendant has not demonstrated that he has been deprived of access to any of the evidence of this matter [1] or prejudiced in any way.

8. In fact, prior to the defendant's expert retention, on July 7, 2000, defense counsel was notified by correspondence that any expert retained should be familiar with EnCase software to facilitate their review of the computer evidence. No objection was raised at that time, nor did the defense ever ask for or suggest different imaging software.

WHEREFORE for the above stated reasons, the government respectfully requests that this honorable Court deny the defendant's motion for access to the defendant's computer.

Respectfully submitted

PAUL M. GAGNON
United States Attorney

By:
Helen White Fitzgibbon
Assistant United States Attorney

[1]Presumably, the defense has made allegations about the quality or handling of the evidence in their "secret" affidavit; the government is obviously in no position to respond to any such allegation(s).

5

Legal Analysis of the EnCase Evidence File

§ 5.0 Overview

The central component of the EnCase methodology is the Evidence File, which contains the forensic bit-stream image backup made from a seized piece of computer media. The Evidence File consists of three basic parts -- the file header, the checksums and the data blocks -- which work together to provide a secure and self-checking "exact snapshot" of the computer disk at the time of analysis. The EnCase Evidence File is unique in that it is a secure, self-verifying and fully integrated forensic image specifically designed as read-only random access data in the context of a computer forensic investigation. Many other imaging tools are backup utilities modified for forensic purposes, and as a result do not contain integrated authentication and verification processes.

This section discusses in detail the major components and functions of the EnCase Evidence File that may be relevant for purposes of authenticating the Evidence File in a court of law.

§ 5.1 Evidence File Format

The EnCase process begins with the creation of a complete physical bit-stream forensic image of a target drive in a completely non-invasive manner. With the exception of floppy and CD-ROM disks, all evidence is acquired by EnCase in either a DOS environment, or in a Windows environment, where a specially designed hardware write-blocking device is utilized. The ability of EnCase to image in Windows in conjunction with a write-blocking device presents several advantages to the examiner, including dramatically increased speed, more flexibility, and superior drive recognition.

The acquired bit-stream forensic image is mounted as a read-only "virtual drive" from which EnCase proceeds to reconstruct the file structure by reading the logical data in the bit-stream image. This allows the examiner to search and examine the contents of the drive in a Windows GUI, all in a completely non-invasive manner. Additionally, the integrated process enables EnCase to identify the exact original location of all evidence recovered from a targeted drive without the use of invasive disk utilities.

Every byte of the Evidence File is verified using a 32-bit Cyclical Redundancy Check (CRC), which is generated concurrent to acquisition. Rather than compute a CRC value for the entire disk image, EnCase computes a CRC for every block of 64 sectors (32KB) that it writes to the Evidence File. A typical disk image contains many tens of

thousands of CRC checks. This means that an investigator can determine the location of any error in the forensic image and disregard that group of sectors, if necessary. The Cyclical Redundancy Check is a variation of the checksum, and works in much the same way. The advantage of the CRC is that it is order sensitive. That is, the string "1234" and "4321" will produce the same checksum, but not the same CRC. In fact, the odds that two sectors containing different data produce the same CRC is roughly one in a billion. The CRC function allows the investigators and legal team to confidently stand by the evidence in court.

In addition to the CRC blocks, EnCase calculates an MD5 hash for all the data contained in the evidentiary bit-stream forensic image. As with the CRC blocks, the MD5 hash of the bit-stream image is generated and recorded concurrent to the acquisition of a physical drive or logical volume. The MD5 hash is calculated through a publicly available algorithm developed by RSA Security. The odds of two computer files with different contents having the same MD5 hash value is roughly ten raised to the 38^{th} power. If one were to write out that number, it would be a one followed by thirty-eight zeros. By contrast, the number one trillion written out is one followed by only twelve zeros. The MD5 hash value generated by EnCase is stored in a footer to the Evidence File and becomes part of the documentation of the evidence.

Throughout the examination process, EnCase verifies the integrity of the evidence by recalculating the CRC and MD5 hash values and comparing them with the values recorded at the time of acquisition. This verification process is documented within the EnCase-generated report. It is impossible for EnCase to write to the Evidence File once it is created. As with any file, it is possible to alter an EnCase Evidence File with a disk utility such as Norton Disk Edit. However, if one bit of data on the acquired evidentiary bit-stream image is altered after acquisition, even by adding a single space of text or changing the case of a single character, EnCase will report a verification error in the report and identify the location where the error registers.

§ 5.2 CRC and MD5 Hash Value Storage and Case Information Header

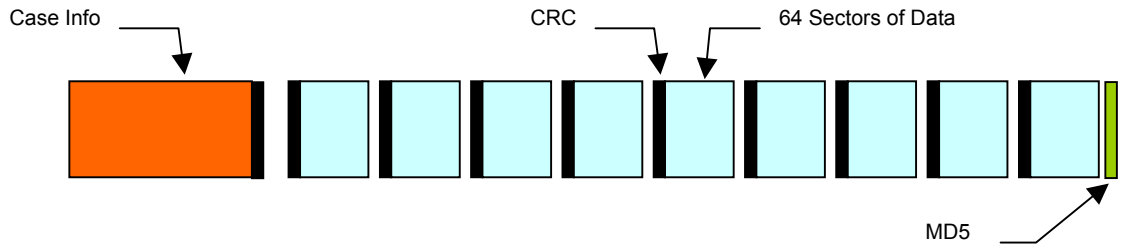


Figure 3: A Graphical Representation of the EnCase Evidence File

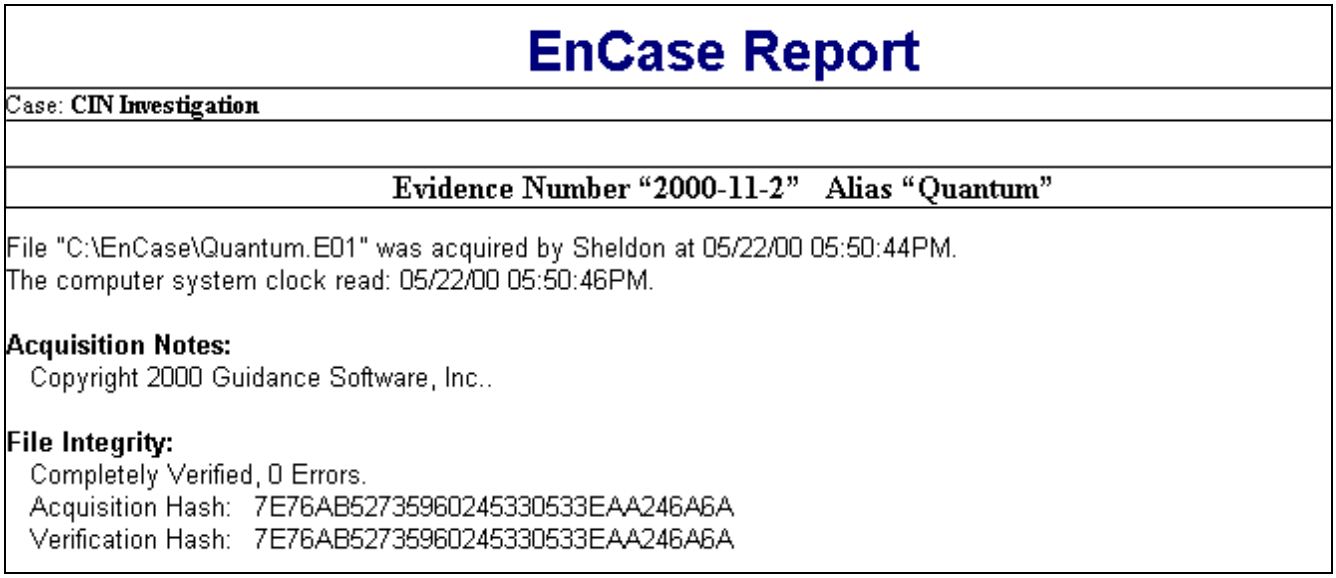
The CRC and MD5 hash values are stored in separate blocks in the EnCase Evidence File, which are external to the evidentiary forensic image itself. Those blocks containing the CRC and MD5 hash values are separately authenticated with separate CRC blocks, thereby verifying that the recordings themselves have not been corrupted. If any information is tampered with, EnCase will report a verification error. Conversely,

merely generating an MD5 hash with another tool and recording it manually or in an unsecured file where it may be altered without detection may not fully insulate the examiner from questions of evidence tampering. For this reason, the CRC and MD5 hash value calculations generated with EnCase are secured and tamper-proof.

The Case Info header contains important information about the case created at the time of the acquisition. This information includes system time and actual date and time of acquisition, the examiner name, notes regarding the acquisition, including case or search warrant identification numbers, and any password entered by the examiner prior to the acquisition of the computer evidence. There is no "backdoor" to the password protection. All the information contained in the Case Info file header, with the exception of the examiner password, is documented in the integrated written reporting feature of EnCase. The Case Info file header is also authenticated with a separate CRC, making it impossible to alter without registering a verification error.

§ 5.3 Chain of Custody Documentation

A distinct advantage of the EnCase process is the documented chain of custody information that is automatically generated at the time of acquisition, and continually self-verified thereafter. The time and date of acquisition, the system clock readings of the examiner's computer, the acquisition MD5 hash value, the examiner's name and other information are stored in the header to the EnCase Evidence File. This important chain of custody information cannot be modified or altered within EnCase, and EnCase will automatically report a verification error if the Case Info File is tampered with or altered in any way.



EnCase Report

Case: **CIN Investigation**

Evidence Number "2000-11-2" Alias "Quantum"

File "C:\EnCase\Quantum.E01" was acquired by Sheldon at 05/22/00 05:50:44PM.
The computer system clock read: 05/22/00 05:50:46PM.

Acquisition Notes:
Copyright 2000 Guidance Software, Inc..

File Integrity:
Completely Verified, 0 Errors.
Acquisition Hash: 7E76AB52735960245330533EAA246A6A
Verification Hash: 7E76AB52735960245330533EAA246A6A

Figure 4: Chain of custody information is documented in an automatically generated report

§ 5.4 The Purpose of Sterile Media and The EnCase Process

Computer forensic investigation procedures developed before the EnCase process require that sterile computer media be used to restore an image backup for analysis by separate search utilities that conduct a physical or "end-to-end" analysis of a single drive. Sterile media is required under such a procedure because the non-integrated disk utilities cannot identify the boundaries of the restored forensic image file. Thus, if an image file of an eight gigabyte drive is restored to a ten gigabyte non-sterile drive filled with data, the two gigabytes of "slack" will be improperly read and analyzed by non-integrated DOS tools. In the past, examiners have experienced problems when utilizing media they believed to be brand new and thus sterile, only to eventually learn that that the storage media was actually only recycled and reformatted. For these reasons, a manually created sterile environment must exist when utilizing search tools that cannot differentiate data residing outside of the original boundaries of the disk image.

The EnCase process does not require the use of sterile media for the same reasons that a word processing program does not require that its text files be stored on sterile media in order to be accurately read. As described above, the EnCase Evidence File is a logical file with logical file boundaries that EnCase recognizes in the same way that MS Word for Windows recognizes a MS Word document. There is no concern that when reading one file, data from another file on the disk will inadvertently bleed onto your screen. As such, the requirement that "sterile media" be used for a computer forensic investigation actually reflects the limitations of the software employed as opposed to being an absolutely necessary item of protocol. EnCase is specifically designed to only read data contained within the Evidence File. As such, there is no possibility that data residing outside of an EnCase Evidence File will be inadvertently searched or analyzed by EnCase.

§ 5.5 Analyzing The Evidence File Outside of the EnCase Process

The EnCase Evidence File is designed not only to contain a forensic image, but a forensic image of a targeted drive that is secured and verified through an integrated process. If an investigator wishes to conduct an analysis of the forensic image contained in the EnCase Evidence File with a tool other than EnCase, the best practice is to restore the physical drive to a separate and dedicated partition before proceeding with the analysis. Otherwise, an investigator may face problems authenticating evidence extracted from an EnCase Evidence File with third party software for several reasons.

First, the CRC and MD5 hash values that EnCase generates and records concurrent to acquisition can only be read and reported by EnCase. The continual verification by EnCase of the integrity of the Evidence File throughout the course of the examination is a key component of the EnCase process. While an MD5 hash of the targeted drive can be independently taken with a separate utility for verification purposes, software operating outside of the EnCase environment cannot confirm the Evidence File data integrity based upon the information recorded by EnCase upon acquisition and stored within the Evidence File. For security reasons, the MD5 hash, CRC values and other case information is secured within the Evidence File and is not designed to be read

by third party software that Guidance Software cannot verify and thus cannot provide testimony regarding its functionality. Further, allowing the EnCase Evidence File to be reverse engineered or “cracked” by third party software is inconsistent with the fundamental principles of computer forensic investigations. EnCase is a carefully designed process specifically for computer forensic investigations and has been widely shown to produce consistent and accurate results. When third party software outside of the design and intent of the EnCase process is utilized, any presumption of authenticity, such as that afforded under Fed.R.Evid. 901(b)(9), may be lost.

Secondly, various acquisition data (investigator's name, dates, passwords, etc), jump tables, file pointers, CRC data and the MD5 hash block are stored either in the Evidence File header or at intervals between blocks of acquired data to allow integrated verification of data integrity and to enhance error detection and speed. While EnCase recognizes this “external” data as outside of the evidentiary forensic image, third party search tools cannot so differentiate and thus will scan this data when running a search directly on an EnCase Evidence File. In other words, these programs may "find" something that was not placed there by the suspect or user. Further, if any such "non-evidentiary" data happens to fall in between blocks of acquired data that make up a picture or document, the evidence will likely not be recovered at all, leading to incomplete results. At best, the investigator will have to repeat the whole exercise in a forensically proper manner.

Another critical factor involves the important EnCase function of identifying the precise location of each byte of data on the original drive. This is an important feature of the EnCase process, as any evidence recovered by EnCase can be independently verified by disk utilities such as the Norton tools when utilizing the precise disk location information automatically provided by EnCase. However, even if data is successfully extracted from an EnCase Evidence file by a third party utility, that tool cannot identify the precise location where that data resided on the suspect's media at the time of acquisition. While it is possible to attempt to manually approximate the location under such a methodology, such a practice is forensically unsound for obvious reasons.

Finally, in the same way that a Zip file’s contents are not readable until "unzipped," raw information on a hard drive or in a forensic image file is not "evidence." It only becomes evidence when it is "mounted" as a file system in the same way that the suspect used it. EnCase reads file system partition tables and fragmentation blocks by analyzing the file system structure (MBR, FAT tables, etc). Only by knowing the "cluster chain" of all the files (and the unallocated areas) can a complete recovery process be possible. By simply conducting a physical "end-to-end" search of the Evidence File, third party utilities ignore this crucial information and therefore cannot attain the complete recovery of data. At worst, the process could result in "splicing" together pieces of unrelated documents and pictures, and thus "creating" evidence in the process.

For the same reasons, EnCase is not designed to mount images created by other proprietary imaging tools, such as a Safeback or Ghost image. In addition to the verification and rule 901(b)(9) issues, there are significant questions whether reverse engineering a proprietary file format constitutes copyright infringement.[90] Further, the concerns regarding infringement raise symmetrical questions about the accuracy of a

process that involves reverse engineering a proprietary image file format without the consent of the developer. Because of such questions, EnCase is not designed to mount or "crack" other proprietary file images.

6

Challenges to EnCase and Other Litigated EnCase Issues

Computer forensic investigators throughout the world utilize EnCase for the seizure, analysis and court presentation of computer evidence. Reports from the field indicate that computer data acquired and processed with EnCase has been successfully admitted into evidence in thousands of trials and preliminary hearings throughout the world. There are no known instances of sustained objections to EnCase-based computer evidence on authentication grounds relating to the use of EnCase. There are to date three particularly notable cases where EnCase withstood challenges over other processes:

1. *Mathew Dickey v. Steris Corporation*, (United States Dist. Ct, Kansas No. 99-2362-KHV)
2. *State of Washington v. Leavell* (Okanogan County, Washington Superior Ct. no. 00-1-0026-8)
3. *People v. Rodriguez* (Sonoma County, California Superior Ct. no SCR28424)

Matthew Dickey v. Steris Corporation

The first known instance of a "serious" challenge to the use of EnCase occurred in a civil litigation matter before the United States Federal District Court, Kansas, where at an April 14, 2000 pre-trial hearing, the court ruled that the testimony of an Ernst & Young expert regarding his computer forensic investigation based upon EnCase would be allowed, overruling objections from the Plaintiff. In *Matthew Dickey v. Steris Corporation*, the trial court overruled evidentiary objections to the introduction of EnCase-based evidence at an April 14, 2000 pre-trial hearing. Plaintiff Dickey brought a motion *in limine* seeking to exclude the testimony of an Ernst & Young expert, regarding the results of his computer forensic investigation based upon the use of EnCase. The Plaintiff's motion was based upon the report of his own expert, which consisted of a critique of the Ernst & Young report.

Steris Corporation ("Steris") successfully opposed Dickey's motion, clearing the way for the expert testimony based upon EnCase. Steris brought its own motion to exclude the testimony of the Plaintiff's expert. Among Steris's arguments was the contention that the Plaintiff's expert was unqualified to provide an expert opinion about computer forensics as, among other reasons, she was admittedly unfamiliar with the EnCase software. The court denied both motions, finding that 1) the challenge to the EnCase process employed by the Ernst & Young expert was without merit, and 2) the testimony of the Plaintiff's expert would not be excluded, although she could be questioned at trial regarding her unfamiliarity with EnCase, which would be relevant to her credibility as a computer forensics expert.

State of Washington v. Leavell

On October 20, 2000 in a Washington State Superior Court, a contested hearing took place in the matter of *State of Washington v. Leavell*[91] where the defense brought an unsuccessful suppression motion to exclude from trial all computer evidence obtained through a forensic investigation utilizing EnCase. A copy of the complete hearing transcript is included as an attachment to this publication.

The defense brought its challenge on two grounds: 1) That the government's examiner could not establish a proper foundation for the evidence, asserting that EnCase was essentially providing "expert testimony" and that the defense was unable to cross-examine the government witness in detail regarding how EnCase works and how it was developed; and 2) That EnCase should be subject to a *Frye*[92] analysis, which is a legal test employed by many courts in the United States to determine whether a scientific technique for obtaining, enhancing or analyzing evidence is generally accepted within the relevant scientific community as a valid process.

The Court ruled that the government's trained computer examiner could provide a sufficient foundation for the evidence recovered by EnCase, and that EnCase met the *Frye* test as a process with general acceptance and widespread use in the industry. On the issue of evidentiary foundational requirements, the Court relied on the case of *State v. Hayden,*[93] which upheld the validity of enhanced digital imaging technology and the admissibility of evidence obtained through this process. The Court noted that like enhanced digital imaging technology, EnCase is merely a tool utilized by the State's examiner and is not providing expert "testimony." The Court determined that the investigating officer who was trained in computer forensics could testify regarding the EnCase process.

On the related argument of the *Frye* analysis, the Court similarly upheld the introduction of evidence obtained with EnCase. The Court determined that EnCase was a widely used and commercially available software tool for recovering computer evidence, including deleted files, and that the investigating officer had conducted his own testing and successfully recovered deleted files on many other occasions. The defense based its *Frye* challenge in part on the theory that only Microsoft could completely and accurately recover deleted files, as the inner workings of the Windows operating system were proprietary. The government countered by producing an affidavit from an internal computer forensic investigator at Microsoft who testified that his department utilized commercially available software for the forensic recovery of deleted files, and that EnCase was one of their primary tools for this purpose. The Court expressly took judicial notice of Microsoft's use of EnCase software, which served as one of the considerations in the Court's ruling.

Finally, the Court relied upon the case of *United States v. Scott-Emuakpor*,[94] which is addressed at length in section 3.1. The court in *Scott-Emuakpor* determined that the United States Secret Service agents who conducted the computer forensic examination did not need to be a qualified experts in computer science to present their

findings and that the USSS agents could provide testimony to authenticate and introduce documents purportedly found on the Defendant's computers.

People v. Rodriguez

On January 11 and 12, 2001 in Sonoma County, California Superior Court, a contested hearing took place in the matter of *People v. Rodriguez*[95] where the court subjected EnCase to lengthy pretrial evidentiary hearing to establish its foundation as a valid and accepted process to recover computer evidence for admission into court. (A copy of the complete hearing transcript is included as an attachment to this publication.) The Rodriguez case involved recovered e-mail messages from defendant Rodriguez's seized computer. Many of the e-mails sent by Rodriguez included his boasts of committing several armed burglaries and robberies. The e-mails were highly relevant to Rodriguez's intent and state of mind.

The defense brought its challenge on two grounds: 1) That EnCase should be subject to a *Frye*[96] analysis, which is a legal test employed by many courts in the United States to determine whether a process for obtaining, enhancing or analyzing scientific or technical evidence is generally accepted within the relevant scientific community as a valid process; and 2) That the EnCase Report itself should not be admitted into evidence. The *Frye* test is employed in state courts, while *Daubert,*[97] a variation of *Frye*, but based upon the same basis principles, is the standard in US Federal court. Many other countries with a common law system also utilize standards with many similarities to a *Daubert* analysis for scientific evidence, but there is no known record of such tests being applied to the concept of computer forensics.

Upon the conclusion of the hearing, the defense conceded that EnCase was an "appropriate and accepted" methodology under the *Frye* test for recovering computer evidence.[98] After finally admitting that EnCase represented a valid and accepted process, the defense then focused its attention on whether the EnCase Report itself should be admitted into evidence, under the grounds that the prosecution could not properly authenticate the document. The court overruled the defense's objection and allowed the EnCase report generated by the examiner into evidence. After the court's ruling, the trial proceeded and the jury ultimately returned a verdict convicting Rodriguez of robbery, burglary and assault with a deadly weapon.

The transcript features an extensive direct examination and a cross-examination of the computer forensic examiner, addressing in detail the factors related to authenticating the EnCase process under a *Frye* analysis. The prosecution testimony in the *Rodriguez* case is very similar to that of the mock trial transcript provided in section 3.2. Among the findings presented in the hearing were that EnCase was a widely used and commercially available software tool for recovering computer evidence, including deleted files, and that the investigating officer had conducted his own testing and successfully recovered deleted files on many other occasions. The extensive peer review and publication of the EnCase software was also emphasized. These points and the widespread acceptance of EnCase in the industry were important factors that successfully authenticated the EnCase process under the *Frye* test.

The *Rodriguez* case represents another example of the Courts subjecting EnCase to a *Daubert/Frye*-type hearing, which is normally applied to determine the validity of scientific evidence. (See section 2.1 for a discussion of *Daubert/Frye* and computer forensics).

People v. Merken

In one notable recent prosecution featuring the EnCase process, *People v. Merken*, case no 1815448 (May 1999 Calif. Sup.Ct., San Francisco), the defendant was charged with possession of child pornography images found on his hard drive. Initially, the defense was told by the prosecution that it could not obtain a copy of EnCase as the software was only available to law enforcement. On that basis, the defense objected to the admission of the evidence obtained with EnCase on fairness grounds, asserting prejudice from being unable to independently duplicate the processing of the computer evidence. As a compromise apparently invited by the court, the defense moved for and obtained an order for "permission" to purchase EnCase and obtain a discovery copy of the evidentiary bit-stream image. The defense subsequently did not challenge the admission of the computer forensic evidence introduced by the prosecution, and in fact relied upon the testimony of their own computer forensics expert, who presented findings from his independent analysis of the discovery image evidence using EnCase.

The *Merken* case is significant as it serves as an illustration where the defense relied upon the EnCase process instead of opposing it. As EnCase allows for a more objective and automated search process that facilitates accuracy and independent duplication, courts should be less inclined to bar electronic evidence on the grounds that its admission would be unfair to the defense.[99]

7

Search and Seizure Issues and EnCase

§ 7.0 Overview

Issues related to the search and seizure of computer data is an area that has seen some excellent research and writing by prosecutors and government attorneys. The Federal Guidelines on Searching and Seizing Computers, found at www.cybercrime.gov, is a must read for every computer investigator. This Journal focuses on the more narrow search and seizure processes that are potentially impacted by the use of EnCase. The plain view doctrine, for example, is an area that becomes more complex as EnCase allows forensic examiners to view, sort and manage many more files than previously possible with command line utilities.

The remote preview function of EnCase also plays an important role in search and seizure issues. Many users report successful employment of the non-invasive EnCase remote preview feature in consent search situations. Obviously, one is more likely to allow the search of their computer if the preliminary exam can be done quickly and without "impounding" their favorite laptop. The feature is also very useful in increasingly common scenarios where the examiner is faced with numerous items of media and/or severe time constraints and can triage the media on the scene, or where a "blind" examination of media potentially containing other privileged documentation is required.

This chapter will focus on the areas of search and seizure law where EnCase impacts many of the procedures and considerations addressed by current case law.

§ 7.1 Computer Files and the Plain View Doctrine

The Plain View Doctrine allows for seizure of evidence without a warrant where (1) the officer is in a lawful position to observe the evidence; (2) the object's incriminating nature is immediately apparent; and (3) the officer has a lawful right to access the object itself.[100] In the context of computer investigations, a "plain view" seizure of a computer file would likely only arise where officers lawfully observed a monitor attached to an operating computer displaying material evidencing criminal activity. However, absent exigent circumstances, clear consent to search the computers themselves, routine border searches[101] or more rare instances of a plain view display of criminal activity on a running monitor, courts have routinely excluded evidence obtained from warrantless searches of computer files.[102] The gray areas typically arise in more common situations where an officer lawfully searching computer files pursuant to a warrant comes upon evidence of criminal activity unrelated to that specified in the warrant. Recent judicial trends indicate that courts are affording special protection to electronic data stored on computers by narrowly construing the articulated terms of the

warrant. In order to understand the Plain View Doctrine in the context of computer files, the related issue of warrant particularity requirements should be understood.

The Fourth Amendment to the United States Constitution requires that all warrants particularly describe the place to be searched and the items to be seized. In order to pass constitutional muster, a warrant (1) must provide sufficiently specific information to guide the officer's judgment in selecting what to seize, and (2) the warrant's breadth must be sufficiently narrow to avoid seizure of purely unrelated items.[103] While courts readily tailor warrants authorizing searches of more traditional items of physical evidence, "computers create a 'virtual' world where data exists 'in effect or essence though not in actual fact or form.'"[104] Ultimately, whether or not computer files containing information not included within the scope of the warrant can be searched often depends upon the specific language of the warrant. Thus, magistrates should ideally strike a careful balance between a warrant that is too overbroad and one that is so narrow as to prevent the search of all items relevant to the investigation. However, due to a computer's ability to store vast amounts of information, the potential difficulty in accessing particular files in a computer, and the fact that the titles of many files do not satisfactorily indicate the substance of that file, it is often difficult to meet the constraints of the Fourth Amendment.[105]

Courts have generally upheld the search of all files contained within a computer where the warrant authorizes a broad search of computer equipment. In *United States v. Simpson*[106] the court found that where a warrant authorized the broad search of a suspect's computer, an additional warrant was not required for the individual computer files. The court noted that, at the time, there was no known authority providing that computer disks and files were closed containers separate from the computers themselves.[107] In *United States v. Upham,*[108] the court held that the recovery of deleted files pursuant to a search warrant authorizing the seizure of "any and all computer software and hardware, … computer disks, disk drives … visual depictions, in any format or media, of minors engaging in sexually explicit conduct [as defined by the statute]" was valid and did not exceed the scope of the warrant.[109] The court noted that from a legal standpoint, the recovery of deleted files is "no different that decoding a coded message lawfully seized or pasting together scraps of a torn-up ransom note."[110]

In cases involving the investigation of child pornography, many courts have ruled that a warrant allowing seizure of a computer and all its associated printing, storage, and viewing devices is constitutional as the computer, applications, and various storage devices not only may contain evidence of distribution of child pornography, but are also the instrumentalities of the crime.[111] In *United States v. Lacy,*[112] the court allowed seizure of the suspect's entire computer system, hardware and software, because "the affidavit in this case established probable cause to believe Lacy's entire computer system was likely to evidence criminal activity."

However, other courts have invalidated warrants found to lack sufficient particularity. In *United States v. Kow,*[113] the court held a warrant to be overbroad as it allowed seizure of computers, computer files and storage devices without any real

limitations in scope such as the criminal conduct being investigated or a time frame within which the alleged criminal activity took place. As such, the court found that the warrant impermissibly permitted the seizure of essentially every computer-generated document relating to the defendant's business.[114] In response to the concerns raised in *United States v. Kow*, most magistrates are now drafting warrants authorizing the search and seizure of computer media with more narrow definitions of the items to be seized. In turn, the latitude of a search is sharply curtailed where the magistrate provides very specific delineations as what is to be seized pursuant to the warrant and what is to be ignored.[115]

§ 7.2 United States v. Carey

The case of *United States v. Carey*[116] is a clear example of where narrowly drafted search warrants prevent any expansion of the search of computer media beyond the scope of that prescribed by the warrant. In *Carey*, officers investigating evidence of drug transactions obtained a warrant to search the defendant's computers. The subject warrant limited the search to the specific purpose of only searching defendant's computer files for "names, telephone numbers, ledgers, receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances."[117] The scope of the search was thus confined to evidence pertaining to drug trafficking. After conducting a series of unsuccessful text string searches for files related to illegal drug activity, the investigating officer noticed other directories with files that he "was not familiar with," which turned out to be .jpg files.[118] Apparently unable to view the .jpg files with the forensic software utility he was using, the officer exported the files to floppy disks and then viewed them on another computer.[119] Upon opening the first file, the officer determined that it contained an image of child pornography. He then, by his own admission, abandoned the original search for evidence of narcotic transactions and instead searched for and seized evidence related to child pornography.[120] The court ruled the officer's actions exceeded the articulated scope of the warrant and thus violated the Fourth Amendment.

The government unsuccessfully argued that the Plain View Doctrine authorized the search of the child pornography files. The government asserted that "a computer search such as the one undertaken in this case is tantamount to looking for documents in a file cabinet, pursuant to a valid search warrant, and instead finding child pornography." The government further contended that "[j]ust as if officers had seized pornographic photographs from a file cabinet, seizure of the pornographic computer images was permissible because officers had a valid warrant, the pornographic images were in plain view, and the incriminating nature was readily apparent as the photographs depicted children under the age of twelve engaged in sexual acts."[121] The warrant authorized the officer to search any file, according to the government, because "any file might well have contained information relating to drug crimes and the fact that some files might have appeared to have been graphics files would not necessarily preclude them from containing such information."[122] At oral argument, the government expounded on the filing cabinet theory, arguing that the situation "is similar to an officer having a warrant to search a file cabinet containing many drawers. Although each drawer is labeled, he had

to open a drawer to find out whether the label was misleading and the drawer contained the objects of the search."[123]

The court rejected the government's argument that the files were in plain view, finding that "it (was) the contents of the files and not the files themselves which were seized." The court also noted that the pornographic images "were in closed files and thus not in plain view."[124] By this language, the *Carey* court seems to imply that file folders evidencing criminal conduct outside the scope of the search warrant may be seized, but the actual file contents may not be searched absent a supplemental warrant. The court also rejected the file cabinet analogy noting that "[t]his is not a case in which ambiguously labeled files were contained in the hard drive directory. It is not a case in which the officers had to open each file drawer before discovering its contents. Even if we employ the file cabinet theory, the testimony of (the officer) makes the analogy inapposite because he stated he knew, or at least had probable cause to know, each drawer was properly labeled and its contents were clearly described in the label."[125] The court further noted that "because this case involves images stored in a computer, the file cabinet analogy may be inadequate. 'Since electronic storage is likely to contain a greater quantity and variety of information than any previous storage method, computers make tempting targets in searches for incriminating information.'(citations) Relying on analogies to closed containers or file cabinets may lead courts to oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage."[126]

The *Carey* court, seizing the opportunity for pontification in an unsettled area of the law, then proposed in *dicta* that courts addressing this issue in future "acknowledge computers often contain 'intermingled documents.' Under this approach, law enforcement must engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant. Where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents. The magistrate should then require officers to specify in a warrant which type of files are sought."[127] In support of its proposal, the court invokes a Harvard Law Review notation, which theorizes that where a warrant "seeks only financial records, law enforcement officers should not be allowed to search through telephone lists or word processing files absent a showing of some reason to believe that these files contain the financial records sought. Where relying on the type of computer files fails to narrow the scope of the search sufficiently, the magistrate should review the search methods proposed by the investigating officers."[128] The court further opines that with "the computers and data in their custody, law enforcement officers can generally employ several methods to avoid searching files of the type not identified in the warrant: observing files types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory. In this case, (the officers) did list files on the directory and also performed a key word search, but they did not use the information gained to limit their search to items specified in the warrant, nor did they obtain a new warrant authorizing a search for child pornography."

However, notwithstanding its extensive comments on the topic and its rejection of the filing cabinet analogy advocated by the government, the court ultimately states that it did not reach its decision on the applicability of the Plain View Doctrine.[129] Instead, the court expressly bases its ruling upon the testimony of the investigating officer who conceded that he intentionally abandoned his search for evidence of drug trafficking and began opening the .jpg files with the intent to search for files containing erotic depictions of minors. Under such circumstances, the court notes, "we cannot say the contents of each of those files were inadvertently discovered."[130] The court indicates throughout the opinion that had the investigating officer obtained a supplemental warrant after viewing the first file containing child pornography, such a supplemental warrant and authorized search would have been proper. The court also implies that had the officer come across the various items of child pornography inadvertently while continuing his search for drug-related information, the Plain View Doctrine would have been applicable. Unlike the majority opinion, concurring opinion is less than subtle on this point, noting that "if the record showed that (the officer) had merely continued his search for drug-related evidence and, in doing so, continued to come across evidence of child pornography, I think a different result would have been required."[131]

§ 7.3 Post-*Carey* Case Law

Several courts have issued published decisions involving the search and seizure of computer media that feature a discussion of *Carey*, while another court has addressed the Plain View Doctrine in the context a forensic text string search of computer files but without a discussion *Carey*. These decisions provide some indications as to the yet undetermined impact of the *Carey* decision.

In *United States v. Gray,*[132] FBI agents executed a search warrant at the home of a suspected computer hacker and seized four computers belonging to defendant, which were taken back to the FBI's offices. The warrant authorized the FBI to search the defendant's computer files for evidence of computer hacking activity, including stolen computer files and utilities enabling unauthorized access to protected computer systems. After imaging the four computer drives onto magneto-optical disks, the FBI Computer Analysis Response Team (CART) agent created a series of CD-ROMs from the disk images to allow the case agents to view the information in readable form. While the information was being copied onto the CD-ROMs, the agent, pursuant to routine CART practice, opened and looked briefly at each of the files contained in the directories and subdirectories being copied to look for the materials listed in the search warrant in the hope that they might facilitate the case agent's search.[133] To accomplish this, the CART agent utilized the CompuPic program to display thumbnail views of the text and graphical image files contained in each directory. In the course of this action, the CART agent came across and opened a subdirectory entitled "Teen" that contained numerous files with ".jpg" extensions.[134] While the agent noted that the files in that subdirectory appeared to contain images of child pornography, he continued his original search pursuant to the warrant.

Thereafter, the agent saw another subdirectory entitled "Tiny Teen," causing the agent to wonder if child pornography resided in that subdirectory.[135] The CART agent testified that he then opened the "Tiny Teen" subdirectory not because he believed it might contain child pornography, which it did, but rather "because it was the next subdirectory listed and he was opening all of the subdirectories as part of his routine search for the items listed in the warrant."[136] Upon determining that the "Tiny Teen" subdirectory did apparently contain child pornography, the CART agent ceased his search and obtained a second warrant authorizing a search of defendant's computer files for child pornography. The search pursuant to the supplemental warrant revealed additional images of child pornography, which, along with the images that triggered the application for the warrant, the defendant moved to suppress.[137]

In upholding the original search and supplemental warrant as lawful, the court noted that:

> "Although care must be taken to ensure a computer search is not overbroad, searches of computer records 'are no less constitutional than searches of physical records, where innocuous documents may be scanned to ascertain their relevancy.' It follows, then, that (the agent's) search of the 'Teen' and 'Tiny Teen' subdirectories was not beyond the scope of the search warrant. In searching for the items listed in the warrant, (the CART agent) was entitled to examine all of defendant's files to determine whether they contained items that fell within the scope of the warrant. In the course of doing so, he inadvertently discovered evidence of child pornography, which was clearly incriminating on its face."[138]

The court found *United States v. Carey* to be distinguishable, finding that the CART agent never abandoned his original search: "he was not commencing a new search when he opened the 'Teen' and 'Tiny Teen' subdirectories, rather, he was continuing his systematic search . . . without regard to file names or suffixes because he was aware that the materials that were the subject of the warrant could be hidden anywhere in defendant's files."[139] The *Gray* court was also unpersuaded by the defense's argument that the CART agent knew the "Teen" and "Tiny Teen" subdirectories did not contain documents or other files related to hacker activity when he searched them because many of the files had ".jpg" extensions, indicating a picture file, and none of the materials covered by the warrant were believed to be pictures. In a strong affirmation of standard practice by many examiners, the court noted that the CART agent "would have been remiss not to search files with a '.jpg' suffix simply because such files are generally pictures files," based upon his experience that computer hackers often intentionally mislabel files, or attempt to bury incriminating files within innocuously named directories.[140]

In *United States v. Scott-Emuakpor,*[141] FBI and Secret Service agents

investigating a bank fraud scheme obtained a warrant authorizing the seizure of "[a]ll documents purporting to offer an investment opportunity regarding Nigerian accounts or contract over-invoicing[,]" and "[a]ll records, including computer files, that disclose the names or addresses of persons solicited for any such investment." In the course of this search of the seized computers, the investigating agents came upon and seized a letter from a third party to the United States Embassy in London applying for a visa on behalf of defendant. The defendant, relying upon *United States v. Carey*, contended that given the warrant's very specific delineations, the letter to the Embassy should have been excluded, as it was not a document that disclosed "the names or addresses of persons solicited for any such investment." The court upheld the search, finding that *Carey* was inapplicable as there was "no evidence that the agents examining the computer equipment knew that any particular file contained evidence of criminal activity other than the Nigerian fraud scheme." The court also determined that the seizure of the Embassy letter was appropriate as related evidence within the scope of the warrant because it tied Defendant to Intercorp and to England, a fact which the Government contended was central to the fraudulent scheme it intended to prove at trial.

In *United States v. Scott,*[142] Secret Service agents conducting a counterfeit securities investigation obtained a warrant authorizing the search of a the suspect's residence and seizure of items that constituted "evidence of criminal offenses, the fruits of crime, and the instrumentalities of criminal offenses."[143] Although the initial warrant did not specifically provide for the seizure of the computer files and equipment, the court held the seizure of two computers was proper as the officers had probable cause to believe the computers were being used as an instrumentality of criminal offenses, and thus the officers acted within the scope of the warrant.[144] In the course of examining the seized computers for information relating to the bank fraud investigation, the investigating agent conducted what the court describes as "a 'text string' mirror-image search of the computers' hard drives."[145] The investigating agent utilized EnCase for this process and his overall computer investigation.[146] The text string search resulted in numerous hits that, in conjunction with other independent information, led the agents to believe that the defendants may have been involved in additional crimes involving bank and tax fraud. On that basis, the agents sought and obtained a supplemental warrant authorizing the search of the computers for evidence of the additional crimes, which the court ultimately found to be supported by adequate probable cause.[147]

In *Wisconsin v. Schroeder,*[148] detectives conducting an investigation of online harassment and disorderly conduct were issued a search warrant to enter the defendant Schroeder's residence and seize his computer and related items in order to search for evidence of his having posted the Internet messages. Upon seizing the computer system, Schroeder indicated to the officers that there was child pornography on his computer. The computer was then sent to the state crime lab for analysis, where the officer who served the warrant informed the computer lab examiners that child pornography might be residing on the computer. In their search for evidence of online harassment, the lab examiners did find some pornographic pictures of children, at which point they stopped their search and sought a second search warrant to provide authority to search for child pornography on Schroeder's computer. Upon being issued the second warrant, the state

crime lab examiners resumed the search and found more illicit pictures of minors, as well as evidence of the online harassment.

Schroeder sought to suppress the evidence of child pornography, asserting that the crime lab's initial discovery of the images did not legitimately fall under the plain view doctrine exception and thus the supplemental warrant represented "fruit of the poisonous tree." Schroeder contended that when the crime lab analyst first began to search the computer for evidence of harassment, he was also actively looking for child pornography even though there was no warrant for him to do so. Schroeder noted that after being told that there might be child pornography on the computer, the crime lab analyst opened files that had names suggestive of child pornography and thus was "verifying" that the files did contain child pornography. According to Schroeder, "This additional step of opening and reviewing the folder to verify it contained child porn makes the search illegal."
The lab analyst testified, however, that when he searches a computer he systematically examines user-created files regardless of their names, in the event that a file has been renamed in order to conceal its contents. While systematically opening all user-created files, the lab analyst opened one containing images that he considered child pornography. At that point, he stopped his search and proceeded to obtain a supplemental warrant. He did not resume his search and find the rest of the contraband until after the issuance of the second search warrant. Thus, his initial discovery of child pornography occurred when he opened a file and saw a nude picture of a child appear on his monitor. Finding that the plain view doctrine did apply, the court noted "this was no different than an investigator opening a drawer while searching for drugs and seeing a nude picture of a child on top of a pile of socks."

The *Schroeder* court placed heavy reliance on *United States v. Gray*, and, like the *Gray* court, distinguished *United States v. Carey*. The Schroeder court noted, "[i]n *Gray*, as in the present case, the investigator stopped searching and obtained a second warrant. There, as here, the continued search for child pornography was authorized by the second warrant."

§ 7.4 Post-*Carey* Practice

In a nutshell, *Carey* provides that an investigator may not manually search through individual files in a concerted effort to obtain information outside a warrant's articulated scope. While not addressing *Carey*, the *United States v. Scott* decision provides an indication that text string searches performed across an entire hard drive or other form of media would not subject the examiner to questions of exceeding the scope of a warrant, as long as such text searches were generally within the course of the investigation delineated by the warrant. By logical extension, results from aggregate hash file analysis, signature mismatch analysis and other automated functions featured in EnCase would provide a means for investigators to justifiably seek supplemental warrants to broaden searches for evidence of additional criminal activity. At the same time, investigators employing such practices would arguably be better insulated from charges that they conducted an unauthorized review of individual files to obtain probable cause for the supplemental warrant. EnCase version 2+ features several additional automated features, such as the categorization of all files in a case into three separate

hash value categories: 1) unknown hash value; 2) known hash value – suspect; and 3) known hash value – non-suspect. Version 2 also features a capability providing for an unlimited number of executable macros and filters, and an automated picture gallery displaying all known graphical images in a case. As these functions will presumably be enacted as a routine practice in the course of computer investigations, supplemental warrants based upon information obtained from the aggregate outputs of these automated processes would be within the scope of the Fourth Amendment. See, *United States v. Gray,*[149] (software providing thumbnail views of all files in a directory properly utilized as standard FBI CART practice).

The *Carey* court proposes that in future investigations, computer examiners should be required to "engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant. Where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents." The court notes that law enforcement computer investigators "can generally employ several methods to avoid searching files of the type not identified in the warrant: observing files types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory." If the courts were to adopt such a "file sorting" requirement, EnCase provides an excellent, if not sole mechanism to comply with various computer file-sorting instructions from a magistrate.

§ 7.5 Warrant Return Requirements

Reports from the field indicate that the majority of federal magistrates are now requiring that computer forensic analysis upon computer media seized from businesses be completed within specified time periods, often 30 days. "A search warrant must be executed and returned to the judge or commissioner who issues it within [the time frame specified in the warrant]; after the expiration of this time the warrant, unless executed, is void."[150] Thus, the failure to complete a computer forensic analysis within the time specified will likely result in the suppression of the evidence found in the course of the investigation. In *United States v. Brunnette*, the court excluded evidence obtained from a computer investigation that was not completed within the 60 day period prescribed by the warrant.[151] Further, as demonstrated by *Steve Jackson Games v. United States*[152] an agency may be exposed to civil liability for unreasonably retaining custody of seized computer media.

This is one area where EnCase presents a double-edged sword for law enforcement. If all federal magistrates were educated as to the capabilities of the software, we would unfortunately see further time constraints being placed upon the analysis of seized computer media. (This is one reason why this publication is privately disseminated). Courts have thus far analyzed this issue in the context of older computer forensic technology noting that "it is no easy task to search a well-laden hard drive by going through all of the information it contains, let alone to search through an the disks for information that may have been 'deleted.'" *United States v. Upham*,[153] (analyzing

forensic processes utilized by U.S. Customs in early 1997, before the agency's adoption of EnCase). The court further states "if the images themselves could have been easily obtained through an on-site inspection, there might have been no justification for allowing the seizure of all computer equipment." In reviewing a 1995 forensic examination, the court in *United States v. Hunter,*[154] opined, "until technology and law enforcement expertise render on-site computer records searching both possible and practical, wholesale seizures, if adequately safeguarded, must occur."

Thus, it is only a matter of time before warrant return requirements of 10 days or less become the standard for computer examinations. A clear example is the Southern District of the 9th Circuit (San Diego) where magistrates are now routinely mandating on-site computer examinations when issuing warrants to be executed at business establishments. Not coincidently, the San Diego Regional Computer Forensics Lab resides in the Southern District of the 9th Circuit, and the capabilities and expertise of the lab are widely known by the local bench.

8

Complying with Discovery Requirements when Utilizing the EnCase Process

§ 8.0 Overview

One of the questions prosecutors and examiners routinely face in the field is complying with discovery requirements when the prosecution's computer evidence is contained within an EnCase image. This is a somewhat difficult issue due to the very nature of computer evidence. Printing out all the data on a typical 10-gigabyte hard drive would result in a stack of paper approximately 300 meters tall. Even worse, this data will be compromised unless properly handled with computer forensic software. The question then becomes — what is required to produce relevant computer evidence in the course of discovery?

There are several models for producing electronic evidence in the course of discovery that are employed by prosecutors and attorneys. Each have their own strengths and weaknesses, and the applicable statutes and discovery rules of the particular jurisdiction and preferences and discretion of the individual judge often determine which of the following models are most suitable.

§ 8.1 Production of Entire EnCase Images

Many attorneys choose to produce exact copies of the EnCase Evidence File, which is a complete physical image of an acquired drive. Often the prosecution will also produce the Case File, which contains the bookmarks, text-string searches, various notes and comments of the investigator, as well as other information. As much of the data contained within the Case File, such as the examiner's bookmarks and notations could be considered work product, it is within the discretion of the prosecutor to produce such evidence. Many prosecutors in the U.S. inform the defense that it should retain an expert who is familiar with the EnCase software. With EnCase and the practice of computer forensics becoming more standard, there are an increasing number of experts in the private sector as well as Federal and State Public Defenders offices who are utilizing the software. As such, this option is becoming increasingly more feasible as the practice of computer forensics expands.

The advantage to this approach is that it ensures the defense cannot tamper with the evidence, at least without detection, and dispels any claim that the prosecution withheld evidence. For these reasons, this method of discovery is the most desirable. The disadvantage to this approach is that many defendants and their counsel still lack the expertise or means to purchase and utilize the EnCase software, although as noted above, this trend is decreasing.

§ 8.2 Production of Restored Drives

Another option is to provide a restored hard drive, which is a complete bootable clone of the original seized drive. EnCase includes a feature that allows the examiner to easily restore an EnCase image to a separate drive. EnCase version 2.11+ will restore the seized drive onto a separate drive and verify the copy by a 128 bit, MD5 hash, which will match that of the original evidence, even if different sized media is utilized in the process. After receiving the discovery, the defense's retained expert can examine the evidence.

The advantage of this approach is that it provides the entirety of the evidence in a manner that most laypersons can access and view. However, the disadvantage of this approach is that deleted, temporary and buffer files, as well as key metadata are not viewable by simply booting the cloned drive. Also, once the defense boots the cloned drive, much of the evidence would change, including date stamps and writes to the swap file. As a result, the Defense may attempt to introduce, and not necessarily by intention, evidence that is not an accurate reflection of the data as it existed at the time the government seized the computer media. Of course, with the MD5 hash of the restored drive recorded, the prosecution would be able to detect that any changes were made to the restored drive by the defense.

§ 8.3 Production of Exported Files

Some prosecutors provide selected exported files and other information from the Evidence File, along with printouts of that information. Production of these files and blocks of selected data is achieved by transferring the information to a CD-ROM disk in a format that is easily viewable by counsel. The EnCase report may also be produced. This option provides the exact information that the prosecution intends to introduce at trial in a convenient and easy to read format. By providing the electronic evidence on CD-ROM disks, the defense cannot tamper with the selected portions of the original evidence. Disadvantages of this process include potential claims that the production was too narrow and that potentially exculpatory documents were omitted. Many courts tend to prefer that document productions be comprehensive, as opposed to more limited productions that may not contain all relevant data.

§ 8.4 Supervised Examination

Where the Defense has retained an expert, another option is to permit the defense expert to access, under supervision of the investigating officer and/or a special master, an image of the original drives so that the expert can conduct a proper and non-invasive investigation. This approach is essentially the only option where the computer evidence consists of contraband, such as child pornography. Ideally, the expert would utilize EnCase to conduct the exam, but may be permitted access to the original drives or a properly restored clone for re-imaging with other non-invasive tools.

Section 4.4 summarizes a New Hampshire Federal District Court case where the prosecution offered to allow the Defense supervised access to a copy of the EnCase Evidence File, which contained images of child pornography. However, the Defense contended that it required access to the original computer systems in question so that they could operate those computers and examine them in their native environment, and filed a formal written request for a Court order allowing such unfettered access to the "original" computer evidence. The Government filed a successful objection to the request, asserting that the "mirror image" created by the Special Agent is the proper way to preserve the original evidence. The Government asserted that merely turning on the computer, as the Defense requested, will change the state of the evidence by altering critical date stamps and potentially overwriting existing files and information.

The Court ruled that the Defense could only have access to the original computer systems if their expert created a proper forensic image under the supervision of the Special Agent. The Defense was barred from booting the original computer systems to their native operating systems.

§ 8.5 Discovery Referee in Civil Litigation Matters

Electronic evidence discovery has recently become a critical component of civil litigation. This has not always been the case as the prior DOS-based, non-integrated methods of computer forensic investigation often proved cost-prohibitive, inefficient and incompatible with the needs of litigation counsel in terms of reviewing the complete investigation results and producing them to the opposing party. In *Alexander v. Federal Bureau of Investigation,*[155] an information technology specialist from the Executive Office of the President testified that the examination of a single hard drive to locate documents responsive to a subpoena (employing non-EnCase methodology) would require approximately 265 hours. If a law firm were to retain an expert to conduct a similar task at an average standard rate of $300 per hour, the cost would nearly exceed $80,000 for the examination alone. It is thus no wonder that the *Alexander* case often found its way into briefs submitted by litigants seeking to quash an adversary's subpoena for the production of computer evidence. As recent as July 1999, counsel advanced the argument in one well-publicized federal litigation that e-mail discovery was "simply not feasible."[156]

Even though civil trial lawyers have long recognized the importance of computer evidence discovery involving the assistance of computer forensic experts, enormous financial constraints generally limited the practice to only the most well financed lawsuits. However, recent significant improvements in computer forensic techniques and software have reversed this trend. Recently, an Indiana U.S. District Court issued an order articulating a well-designed discovery protocol for the examination of computers to recover relevant documents, including deleted files. In *Simon Property Group v. mySimon, Inc*.,[157] the court issued an order appointing Seattle-based Computer Forensics, Inc., (CFI) as an officer of the court and directing that CFI generate mirror images of 8 designated computers. The Court issued the order after the Plaintiff brought a motion to compel access to computers in the possession of defendants, who objected to making

their computers available for forensic analysis. The following are some key portions of the *Simon Property* Court's order:

- The Court first ordered the plaintiff to select and agree to pay a computer forensics expert to serve as an officer of the court and ordered the defendants to identify all computers in question that may contain relevant documents. The Court also instructed the parties to meet and confer to draft a proposed order addressing the various details of the inspection process, objections and the transfer of information.

- When the parties failed to agree on a framework, the Court ordered that CFI would carry out the inspection and copying of data from defendant mySimon's designated computers. The Court instructed that all communications between CFI and plaintiff's counsel take place either in the presence of defendant's counsel or through written or electronic communication with a copy to defendant's counsel.

- The Court mandated that within 14 days of the order CFI was "to inspect defendant's designated computers and create an exact copy or 'snapshot' of the hard drives of those computers." The Court noted that the inspection order did not apply to mySimon's computers and servers that actually provide defendant's Internet shopping services and instructed that the inspection be carried out in a manner minimizing disruption of and interference with mySimon's business, and that mySimon and its counsel shall cooperate in providing access to the designated computers.

- The Court mandated that within 28 days of the order CFI: 1) "recover from the designated computers all available word-processing documents, incoming and outgoing electronic mail messages, PowerPoint or similar presentations, spreadsheets, and other files, including but not limited to those files that were 'deleted'" from the 8 separate computers designated by defendants; 2) "provide such documents in a reasonably convenient form to defendant's counsel, along with, to the extent possible, (a) information showing when any recovered 'deleted' files were deleted, and (b) information about the deletion and the contents of deleted files that could not be recovered."

- The Court ordered that within six weeks of the order; 1) CFI "shall file a report with the court setting forth the scope of the work performed and describing in general terms (without disclosing the contents) the volume and types of records provided to defendant's counsel," and; 2) mySimon's counsel shall review the records for privilege and responsiveness, shall appropriately supplement their response to discovery requests, and shall send by overnight delivery to plaintiff's counsel all responsive and non-privileged documents and a privilege log reflecting which documents were withheld pursuant to the attorney-client privilege or work product

immunity.

- The Court also directed that within 30 days after the final resolution of the case, CFI shall destroy the records copied from the designated computers and shall confirm such destruction to the satisfaction of mySimon.

Simon Property demonstrates that a large-scale computer forensic analysis can be performed within a reasonable period of time. Unlike the *Alexander v. F.B.I.* case, the EnCase process is being utilized to carry out the order of the *Simon Property* court.[158] Additionally, the appointment of a single computer forensic consulting firm to act as special master is another important recent trend in civil litigation that better serves judicial economy and efficiency. The alternative of each party retaining separate partisan computer forensic experts only invites prolonged litigation through objections and extensive motions, whereas a single expert acting as special master can expedite the process by retaining custody of the evidence while providing the producing party an orderly means to address any claims of privilege. Further, with the computer forensic expert serving as a special master or officer of the court, any attorney-client or other privileges would not be waived by virtue of a mirror image of the drives being made.

The *Simon Property* case also illustrates that accessing a computer system in question may involve several months of legal wrangling, with critical evidence possibly being overwritten in the meantime. As such, the following are some practice points that counsel should consider when it becomes clear that computer evidence is relevant to a case at hand.

- Issue a demand letter requesting preservation of all relevant computer evidence. An example form of a preservation letter is included below.
- Consider immediately proposing a stipulation to the opposing party along the lines of the *Simon Property* case. Such a measure would immediately enable an expert to access and image the computers in question and retain sole custody of the forensic evidence until the opposing party has had a full opportunity to review documents identified by the expert as relevant and address any objections with the court.
- Any proposed stipulation should include a provision that the parties preserve the integrity of all evidence contained on computer systems in the interim period prior to the inspection by the computer forensic experts. (*See*, *Illinois Tool Works, Inc. v. Metro Mark Products, Ltd*[159]). Ideally, preserving the integrity of the computer evidence means that the computers are not operated at all. While parties will invariably consider such a provision to be burdensome, this underscores that the relevant computer systems should be immediately identified and imaged at the outset of the litigation.
- If the opposing party is uncooperative, the court could consider evidentiary and/or monetary sanctions if an order similar to what you originally proposed for a stipulation is ultimately adopted after a noticed motion.

- Any objections to producing computers for inspection on burden or cost under the grounds set forth in *Alexander v. F.B.I.* should be countered with a discussion of more recently available computer forensic tools that provide significantly increased efficiency to the process.
- In particularly sensitive cases, counsel should consider bringing an *ex parte* motion for a temporary restraining order preventing the operation of relevant computer systems until they can be accessed and imaged.
- A disadvantage to the special master approach is that counsel seeking the discovery may never have the opportunity to review the EnCase evidence file created by the special master expert to search for relevant information that the expert may have missed. Consider seeking permission from the court to obtain a copy of the evidence file for your own review and analysis.

§ 8.6 Example Form Letter Demanding Preservation of Computer Evidence

Below is an example of the type of letter that should be utilized in the context of civil litigation in order to establish a duty and obligation on the part of the recipient to retain and preserve the identified electronic evidence.

<DATE>

_____
_____
_____

Re: **Jane Doe v. XYZ Company**

Dear Sir or Madam:

As critical evidence in this matter exists in the form of electronic data contained in the computer systems of XYZ Company, this is a notice and demand that such evidence identified below in paragraphs 2 through 6 must be immediately preserved and retained by XYZ Company until further written notice from the undersigned. This request is essential, as a paper printout of text contained in a computer file does not completely reflect all information contained within the electronic file. Additionally, the continued operation of the computer systems identified herein will likely result in the destruction of relevant evidence due to the fact that electronic evidence can be easily altered, deleted or otherwise modified. The failure to preserve and retain the electronic data outlined in this notice constitutes spoliation of evidence and will subject XYZ Company to legal claims for damages and/or evidentiary and monetary sanctions.

1. For purposes of this notice, "Electronic Data" shall include, but not be limited to, all text files (including word processing documents), spread sheets, e-mail files and information concerning e-mail (including logs of e-mail history and usage, header information and "deleted" files), internet history files and preferences, graphical image format ("GIF") files, data bases, calendar and scheduling information, computer system activity logs, and all file fragments and backup files containing Electronic Data.

2. Please preserve and retain all Electronic Data generated or received by _____.

3. Please preserve and retain all Electronic Data containing any information about _____.

4. XYZ Company must refrain from operating (or removing or altering fixed or external drives and media attached thereto) standalone personal computers, network workstations, notebook and/or laptop computers

operated by _____.

5. XYZ Company must retain and preserve all backup tapes or other storage media, whether on-line or off-line, and refrain from overwriting or deleting information contained thereon, which may contain Electronic Data identified in paragraphs 2 through 4.

6. In order to alleviate any burden upon XYZ Company, the undersigned is prepared to immediately enlist the services of a computer forensic expert to properly and non-invasively create back-up images all drives and media in the custody and control of XYZ company that may contain Electronic Data relevant to this matter. This can be accomplished through a stipulation setting forth a similar procedural framework outlined by the Court in *Simon Property Group v. mySimon, Inc*. 94 F.R.D. 639 (SD Ind. 2000), to ensure retention of all privileges while properly preserving and processing computer evidence as mandated by the court in *Gates Rubber Co. v. Bando Chemical Indus., Ltd* 167 F.R.D. 90, 112 (D.Col., 1996).

Please contact me if you have any questions regarding this request.

Sincerely,

_____

9

Employee Privacy and Workplace Searches of Computer Files and E-mail

§ 9.0 Overview

Electronic mail is all but firmly established as the primary form of workplace communication. In recent years, employment litigation and other cases involving alleged workplace misconduct routinely involve evidence in the form of e-mail or other computer-generated records created in the course of business. With most of a typical company's "documents" and other information existing in electronic form, employer monitoring, and in many cases, seizure of these files is becoming commonplace. In considering employee privacy in the context of monitoring of e-mail and other computer files, it is important to note that the rights of government employees may differ in many aspects from their counterparts in the private sector. For instance, the United States Constitution's Fourth Amendment restrictions on unreasonable searches and seizures afford potential additional protections for government employees who are subject to monitoring of their e-mail and computer files. As the Fourth Amendment only acts as a check on government actions,[160] the scope of the Amendment's protections for government workers' e-mail is limited, if at all, in application to non-government workers. Conversely, employer manuals and other written information setting forth company policy largely govern privacy rights in the commercial workplace. As such, workplace privacy issues in the private and public sector are addressed separately in this section.

§ 9.1 Employee Monitoring in the Private Sector

While an employer is generally prohibited by law from intercepting e-mail messages being transmitted over the internet,[161] monitoring employee e-mail, stored computer files, including Internet history files, are generally permitted in most states without written consent or notification. Connecticut, a notable exception, requires employers to obtain written consent from their employees before any such monitoring can take place.[162] A bill for a similar statute, dubbed the "Notice Electronic Monitoring Act" (S.2898) was introduced in Congress in July 2000, but as of June 2001 remains in committee. Counsel should remain vigilant in monitoring any developments in the law at both the state and federal level.

In considering the propriety of employer monitoring of employee e-mail and computer files, the primary question concerns whether and to what extent written agreements and policies addressing such monitoring are in place. Written notification that their e-mail and computer files are subject to access by the employer generally governs whether an employee can claim a reasonable expectation of privacy in those files. These

rules, in the form of written e-mail, Internet use and stored computer file policies, must limit the employees' privacy expectations in their electronic communications and stored computer files, but must do so consistently with laws that prohibit interceptions of electronic communications in transit. Moreover, it is important that these rules and polices are expressly acknowledged and consented to in writing by the employee.

Balancing of Interests

In determining an employee's privacy interests, the courts will balance the employer's interest against the reasonable privacy rights of the employee. Preventing theft of intellectual property and policing unauthorized activity are generally seen as compelling interests justifying an employer's reasonable monitoring activities.[163] Additionally, employers may potentially be held liable for an employee's online misconduct where the company's computer networks are the means for the offense.[164] Some legal experts have hypothesized that where an employee utilizes an employer's computer systems to engage in such activities as hacking, on-line harassment or copyright infringement, an employer may be liable for those activities.[165] In the very recent case of *Blakey v. Continental Airlines,*[166] the New Jersey Supreme Court found that Continental Airlines could be potentially liable for an employee's harassing postings on an internet bulletin board hosted by the airline for its employees. In reversing a lower court's order dismissing Blakey's complaint, the Court reasoned that since the company provided the Internet forum for employees' use, Continental had a duty to monitor e-mail postings to ensure that employees were not harassing one another. In another leading decision in this area, *Smyth v. Pillsbury Co*., the Pennsylvania U.S. District Court determined that "a company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments."[167] Thus, with the employers' interest in preventing theft and unauthorized activity coupled with the possibility of third liability for *failing* to monitor the employees' on-line conduct usage, e-mail and Internet usage monitoring of employees is a critical, if not mandatory necessity for employers in the private sector.

§ 9.2 The Electronic Communications Privacy Act of 1986

The Electronic Communications Privacy Act of 1986 (ECPA) is a federal statute that some contend has application to an employer's workplace e-mail monitoring activities. The ECPA includes two categories relevant to this discussion: Title I prohibits interception of messages in transit,[168] while Title II prohibits access to and disclosure of stored information. The "stored information" provision under title II has been narrowly construed to only apply to information in intermediate storage incident to transmission, such as an e-mail residing on a server prior to being retrieved by the recipient.[169] Thus, the ECPA prohibits three types of intrusions into electronic communications: intercepting messages while they are in transit, accessing information in intermediate storage incident to transmission, and disclosing information at any point in the process.[170] While the ECPA may seem to provide employees with broad protection from e-mail monitoring, the Act contains several exceptions that sharply limit its scope. First, it is apparent that

Congress did not intend the ECPA to govern the relations of employees to their employers, but rather intended to regulate intrusions by unauthorized outsiders into the electronic communications of organizations. As such, most commentators believe that the ECPA does not cover workplace local area networks (LANs) and thus provides no protection for employees when they send e-mail over their workplace computer network.[171] The language in the ECPA prohibiting disclosure of electronic communications only applies to those entities that provide electronic communication services "to the public,"[172] while intra-office networks offer services only to employees. Thus, under this construction of the ECPA, any e-mail sent by employees over a nonpublic network would not be subject to the Act.

Second, even if the ECPA did apply to proprietary LANs, the Act contains an exemption allowing access to stored communications when authorized by the entity providing electronic communications services.[173] On its face, this provision allows the network provider to access any stored communication that had been sent over the network without violating the ECPA. If an employer owns the network, it could then access all communications sent by employees. In *Bohach v. City of Reno,*[174] the plaintiffs, two police officers, sought an injunction preventing the City from continuing an internal affairs investigation. In rejecting the plaintiffs' claim that the investigators' violated the EPCA by retrieving the plaintiffs' pager messages stored on the City's telephone network, the court noted that the City was the provider of the electronic communications service used by the officers.[175] It then held that "[section] 2701(c)(1) allows service providers to do as they wish when it comes to accessing communications in electronic storage. Because the City is the provider of the 'service,' neither it nor its employees can be liable under § 2701."[176]

Employers should be aware that actually intercepting e-mail messages in transit, as opposed to accessing stored communications, would likely constitute a violation of the ECPA.[177] Interception is generally defined as the act of accessing a message or preventing it from reaching its destination at any point between the time the message is sent and the time the intended recipient receives it. To date, most courts have taken a narrower view of what constitutes "interception" of e-mail, establishing that under the ECPA, interception can only occur during the fraction of a second the message is actually traveling along the wires connecting computers.[178]

Fraser v. Nationwide Mutual Insurance Co.[179] is the latest case to hold that an employer's retrieval of an employee's e-mail from post-transmission storage does not constitute an "interception" under the ECPA. In *Eagle Investment Systems Corporation v. Tamm*,[180] the court similarly determined that no "interception" occurred when an employee obtained a stored e-mail from a co-worker without his consent.

In *Steve Jackson Games, Inc. v. United States Secret Service*, the Fifth Circuit addressed the issue of whether the seizure of a computer storing private e-mail that had been sent to an electronic bulletin board but not yet read by the recipients constituted an "intercept" proscribed by Title I of the ECPA. The court determined that such a seizure was not an interception because the e-mail was not being transferred but was instead in

storage incidental to transmission.[181] Other courts have reached similar conclusions regarding the definition of interception as used in the ECPA.[182] However, at least one court in a more recent decision has determined that the viewing of information from a secure web page in intermediate storage prior to being read by its intended recipient constitutes an "interception."[183] As such, there is an apparent split in authority regarding whether seizing an e-mail while in intermediate storage incident to transmission and before it is retrieved by its intended recipient constitutes an "interception" under Title I of the ECPA. However, the seizure of e-mail that has been retrieved by its intended recipient is clearly not an interception under the current status of the law.

§ 9.3 Other Important Considerations for Employers

The issue of employee monitoring is complex and the employers should seek the advice of their counsel when considering the implementation of a written policy governing these issues. The following are some additional important considerations for employers:

- Employers should monitor all developments in this rapidly developing area of law. In addition to the Connecticut statute,[184] the California legislature recently passed a law that would have mandated an employee's written consent among other requirements before an employer could monitor their employees' e-mail, Internet usage and stored computer files.[185] Only the somewhat unexpected veto of Governor Gray Davis blocked the enactment of the statute. Similar bills are being considered in other states and in the US Congress.
- In any event, employers should ensure that all employees are informed and consent in writing to any such monitoring activities. Currently in the US, proper written consent provides an exception to almost all existing laws governing employers' electronic monitoring activities.
- Employers and their counsel should be mindful of recent cases that hold employers liable for the wrongful conduct committed by an employee through the internet/network. This adds to the equation of the employer's interests of not only protecting their intellectual property and internal resources but also being charged with a duty to prevent wrongful on-line conduct of their employees.
- Employers should be consistent and even-handed in their monitoring activities in order to avoid common law invasion of privacy claims. An employee could in theory state a claim for improper monitoring if an ordinary reasonable person would find that the circumstances involved "a substantial and highly offensive invasion of privacy."[186] For instance, a targeted, non-routine search for incriminating electronic documents to provide a pretext for the termination of an employee may be construed as unreasonable by some courts.

§ 9.4 Monitoring of Government Employees

Federal, state, and municipal employers constitute a very large sector of the U.S. economy, and the federal government has established a goal of providing e-mail to every federal agency and promoting e-mail as the preferred method of conducting government business. In addition, the federal government has instituted an aggressive telecommuting program, which has encouraged extensive use of e-mail.[187] Included within these aggressive plans for digitizing the federal workplace are equally aggressive e-mail monitoring programs.[188] Unlike their private sector counterparts, federal employees are afforded a degree of protection under the Fourth Amendment's prohibition against unreasonable search and seizures.[189] However, those protections can also be substantially limited by the implementation of written policies and agreements that reduce an employee's reasonable expectations of privacy.[190]

United States v. Simons,[191] is a notable recent case that directly addresses issues of the monitoring and seizure a federal employee's computer files in the workplace. In *Simons,* systems administrators of the Foreign Bureau of Information Service (FBIS) division of the CIA searched an employee's hard drive over a remote network connection after routine network monitoring detected unauthorized Internet connections from his computer to sex-related websites. The FBIS previously instituted a written policy regarding Internet usage by employees stating that employees were to use the Internet for official government business only. The policy specifically prohibited accessing unlawful material and stated that "[u]sers shall . . . [u]nderstand FBIS will periodically audit, inspect, and/or monitor the user's Internet access as deemed appropriate." The record reflects three distinct levels at which FBIS, and then the CIA Office of the Inspector General (OIG), searched and ultimately seized Simons' computer files. First, FBIC investigators performed text searches across the network, resulting in numerous sex-related keyword "hits" originating from Simons' computer. The FBIC network administrator then remotely accessed and copied files from Simons' computer to determine the existence of unauthorized downloaded Internet files. After determining that some downloaded images appeared to be child pornography, investigators from the CIA OIG directed Simons' hard drive be seized from his office without a warrant, despite their knowledge that Simons' computer likely contained images of child pornography.

Simons contended on appeal from his conviction that the FBIS's search of his computer files stored on his hard drive in his office over the network violated the Fourth Amendment. Simons further contended that the OIG's warrantless seizure of his hard drive also violated the Fourth Amendment. The court found the remote network searches of Simons' computer to be proper because, in light of the Internet policy, Simons lacked a legitimate expectation of privacy in the files downloaded from the Internet. Notably, the appellate court declined to recognize any privacy distinction between the network-wide keyword text searches (which Simons did not contest) and the subsequent remote search and seizure of files contained on Simon's hard drive (which Simons objected to).[192]

As far as the entry into Simons' office to seize his hard drive, the court found that

as Simons did have a reasonable expectation of privacy in his office, the warrantless entry and seizure of Simons' computer potentially violated the Fourth Amendment absent the applicability of a specific exception to the warrant requirement.[193] While the FBIS's written policies addressed internet usage and network monitoring, the court found that the policies did not sufficiently address privacy expectations regarding computer files stored on the hard drives and other media actually contained within the employee's office.[194] However, citing the U.S. Supreme Court decision of *O'Connor v Ortega, supra,* the court held that a government employer's interest in "the efficient and proper operation of the workplace" justified the warrantless work-related search of Simons' computer, especially since the *O'Connor* Court held that when a government employer conducts a search pursuant to an investigation of work-related misconduct, the Fourth Amendment will be satisfied if the search is reasonable in its inception and its scope. A search normally will be reasonable at its inception "when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct."[195] Such searches will be considered permissible in its scope "when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of ... the nature of the [misconduct]."[196]

Obviously, the best practice for an investigator in this situation would be obtain a warrant, if feasible, prior to physically seizing a government employee's computer, as courts outside of the Fourth Circuit may not reach many of the conclusions of the *Simons* Court. Further, this case illustrates the importance of comprehensive written policies that not only address e-mail and network activity monitoring, but also the access of stored files on the employee's computer.

NOTES

[1] U.S. Federal Rule of Evidence 1001(1); Canada Evidence Act, Chapter C-5 sections 30(12), 31.8(b).
[2] Canada Evidence Act, Chapter C-5 section 31.1.
[3] *United States v. Siddiqui* 235 F.3d 1318 (11th Cir 2000) (Testimony of recipients sufficient to authenticate e-mails sent by defendant.)
[4] *Authentication of Computer-Generated Evidence In the United States Federal Courts*, (1995) 35 IDEA:J.L.& Tech. 437, 439.
[5] 200 F.3d 627 (9th Cir. 2000),
[6] *United States v. Tank, supra*, 200 F.3d at 629
[7] *Id.* at 630
[8] *Id., citing United States v. Black*, 767 F.2d 1334, 1342 (9th Cir.1985)
[9] *Id.* at 631
[10] *Id.*
[11] See also, *United States v. Whitaker* 127 F.3d 595, 601(7th Cir 1997).
[12] 2000 WL 288443, (W.D. Mich. 2000)
[13] 167 F.R.D. 90 (D.C. Col., 1996)
[14] *Gates Rubber Company*, *supra*, 167 F.R.D. at 112.
[15] *Id*.
[16] 127 F.3d 595 (7th Cir.1997)
[17] *Whitaker, supra,* 127 F.3d at 600-601.
[18] *Id*. at 600
[19] *Id*.
[20] (1988) 205 Cal.App.3d 632
[21] *People v. Lugashi, supra*, 205 Cal.App.3d at 636
[22] *Lugashi,* at 641
[23] *Id.*
[24] *Lugashi,* at 640
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] (1999) 55 Conn.App. 384, 739 A.2d 311
[29] (1997) 949 S.W.2d 93
[30] *Id*. at 100
[31] *Id*. at 97
[32] *Id*. at 99
[33] (1997) 945 P.2d 367
[34] *Id.* at 368.
[35] *Id* at 370
[36] *id*
[37] (1995) 908 S.W.2d 598.
[38] 829 F.2d 757 (9th Cir.1987)
[39] *Id*. at 759
[40] Additionally, *Lugashi* is clearly an important case when seeking to introduce computer-generated evidence created or maintained by third party ISPs, businesses and other institutions.
[41] *United States v. Tank*, 200 F.3d 627 (9th Cir. 2000); *Wisconsin v. Schroeder* 2000 WL 675942
[42] *United States v. Bonallo*, 858 F.2d 1427, 1436 (9th Cir. 1988); See also, *United States v. Glasser*, 773 F.2d 1553 (11th Cir. 1985) ("The existence of an air-tight security system [to prevent tampering] is not, however, a prerequisite to the admissibility of computer printouts. If such a prerequisite did exist, it would become virtually impossible to admit computer-generated records.").
[43] *United States v. Tank*, supra, at 631 fn. 5
[44] *Wisconsin v. Schroeder* 2000 WL 675942
[45] See Bonallo, 858 F.2d at 1436.
[46] 509 U.S. 579, 113 S.Ct. 2786, 125 L.Ed.2d 469 (1993)
[47] *Frye v. United States*, 293 F. 1013 (D.C.Cir.1923).

[48] See, *United States vs. Beasley*, 102 F.3d 1440, 1448 (8th Cir. 1996) (judicial notice taken of reliability of the PCR method of DNA typing).
[49] No. 99-2362-KHV, (D. Kansas)
[50]526 U.S. 137, 119 S.Ct. 1167 (1999)
[51] *Daubert, supra*, 509 U.S., at 592-594, 113 S.Ct. 2786.
[52] See discussion at See, e.g., *United States v. Liebert,* 519 F.2d 542, 547 (3rd Cir. 1975) (holding that computer evidence was admissible in criminal trial provided that prosecution lays a sufficient foundation to warrant a finding that such information is trustworthy and the defense is given the same opportunity to inquire into the accuracy of the computer system involved in producing such evidence). *United States v. Weatherspoon,* 581 F.2d 595, 598 (7th Cir. 1978) (same)

[53] *SC Magazine*. April 2001. "Test Center- GETTING THE HARD FACTS." Testing of Computer Forensics analysis tools reported in the leading publication in the IT Security industry. EnCase receives the highest rating over the other tested programs, noting "If you work doing forensic analysis of media on a regular basis, you must have this tool."

[54] In addition to the recent *SC Magazine* test review noted in fn 7, EnCase has received favorable reviews and mentions in industry publications, including the following articles:

1. IEEE Computer Society, *Computer Magazine* January 2001; "EnCase: A Case Study in Computer-Forensic Technology." A case study on the EnCase process in a leading computer industry journal.
2. *Los Angeles Times*, page A1, October 29, 2000 "High-Tech Snooping All in Day's Work." Front page story on Computer Forensics where EnCase receives favorable and sole mention as the industry leading computer forensic tool.
3. *Information Security Magazine* March 2000; "DDoS and Computer Forensics." Cover Story on Computer Forensics where EnCase is recommended over other commercially available tools.
4. *SC Magazine*. April 2000. "Investigators Focus on Foiling Cybercriminals." Cover Story on Computer Forensics where EnCase receives favorable and sole mention as an industry leading computer forensic tool.
5. *Blue Line Magazine*, November 1999, "A Computer Forensic Utility That Does It All." A favorable and thorough evaluation by a Toronto Police detective who compares EnCase very favorably to the methodologies associated with DOS tools.
6. *Washington Post,* Business Technology Section, April 2, 2000, "Cyber Sleuths Needed." Story on Computer Forensics where EnCase receives favorable and sole mention as the industry leading computer forensic tool.
7. *National Journal's Technology Daily*, January 27, 2000; "Software is the New Tool for Catching Crooks." Story on Computer Forensics where EnCase receives very favorable and sole mention as the industry leading computer forensics tool.

Links to these articles may be found on the Newswire section of Guidance Software's website.

[55] Sonoma County, California Superior Ct. no SCR28424
[56] *SC Magazine*. April 2001. "Test Center- GETTING THE HARD FACTS."
[57] *Daubert*, 113 S.Ct. 2797, 125 L.Ed.2d 483
[58] *State of Washington v. Leavell* (Okanogan County, Washington Superior Ct. no. 00-1-0026-8)
[59] Judicial Notice is the act of a court recognizing the existence and truth of certain facts relevant to the case at bar. Such notice excuses a party from having the burden of establishing fact from necessity of producing formal proof.
[60] "Thus, evidence describing, for example, the process of creating x-rays, photographs, tape recordings, computer generated records, radar records, or scientific surveys when coupled with evidence showing that a particular process or system produces an accurate result when correctly employed and properly operated and that the process or system was in fact so employed and operated constitutes sufficient evidence that the result is what it purports to be." Wright & Miller, Fed.Prac.& Proc. Evid. § 6830; *Notes of the Advisory Committee* regarding Rule 901(b)(9); *see also*, *People v. Lugashi* (1988) 205 C.A.3d 352 (Data collection software program presumed accurate); *People v. Mormon* (1981) 97 Ill.App.3d 556, 422 N.E.2d 1065, 1073 (Data retrieval program presumed accurate) 17 J.Marshall Jour. Of Computer & Info. Law 411, 507-508 [Westlaw: 17 JMARJCIL 411]

[61] 526 U.S. 137, 119 S.Ct. 1167 (1999)
[62] An excellent discussion of this debate can be found at 31 *Federal Practice and Procedure* § 7114 Wright & Miller, (2000 Revision), where the authors identify an apparent conflict between the application of *Daubert* and 901(b)(9).
[63] *United States v. Downing* 753 F.2d 1224, 1240, fn. 21, (3rd Cir. 1985)
[64] 127 F.3d 595 (7th Cir.1997)
[65] *United States v. Whitaker, supra,* 127 F.3d at 600
[66] 18 F.3d 1461 (9th Cir. 1994)
[67] *United States v. Quinn, supra,* 18 F.3d at 1465
[68] *Id.*
[69] 802 S.W.2d 429 (Tx. Ct. App. 1991),
[70] *Burleson v. State, supra,* 802 S.W.2nd at 441.
[71] 71 Am.Jur. Trials 111 (1999) § 118.
[72] *Weisman v. Hopf-Himsel, Inc*., 535 N.E. 2d 1222, 1226 (Ind. Ct. App. 1st Dist. 1989); *People v. Bovio* 455 N.E.2d 829, 833 (Ill. App 1983); *Burleson v. State*, *supra,* 802 S.W.2d at 441; *People v. Lombardi 711 N.E.2d 426* (Ill. App 1999).
[73] *United States v. Liebert,* 519 F.2d 542, 547 (3rd Cir. 1975); *United States v. Weatherspoon,* 581 F.2d 595, 598 (7th Cir. 1978).
[74] *supra*, 2000 WL 288443
[75] 2000 WL 894679 (D.Me.)
[76] See fn. 53,54 for a listing of published papers.
[77] 200 F.3d 627, 630-631 (9th Cir 2000)
[78] 135 F.Supp 207, fn. 1. (2001 D.Me.) According the prosecutor in *Dean*, EnCase was used in the examination and provided an effective means for presenting the results of the examination at trial.
[79] *Fed. R. Evid*. 1002
[80] *Fed. R. Evid*. 1001(1)
[81] The treatise *Overly On Electronic Evidence in California*, (1999) § 9.02; 9-3, comments on California Evidence Code section 255, an identical statute to Rule 1001(3), noting "The approach adopted in Evidence Code section 255 allows for the possibility that multiple or, even, an infinite number of originals may exist. Each time an electronic document is printed, a new 'original' is created."
[82] *Broderick v. State* (2000) 35 S.W.3d 67.
[83] Section V.D.1, citing, *Doe v. United States, 805 F. Supp. 1513, 1517 (D. Hawaii. 1992)*
[84] 1 F.3d 1274 (D.C. Cir 1993)
[85] *Armstrong v. Executive Office of The President, supra,* 1 F.3d at 1280
[86] *Id.* (See also, *Recovery and Reconstruction of Electronic Mail as Evidence* (1997) 41 AMJUR POF 3d 1 §19 ["If the document is a computer printout of an e-mail message, the proponent is required to prove that the printout accurately reflects what is in the computer."])
[87] 135 F.Supp.2d 207, fn. 1. (D.Me.) According the prosecutor in *Dean*, EnCase was used in the examination and provided an effective means for presenting the results of the examination at trial.
[88] 960 F.Supp. 498, 501 (D.Mass. 1997)
[89] 111 F.Supp.2d 294 (S.D.NY 2000)
[90] *Whelan Associates, Inc. v. Jaslow Dental Laboratories, Inc.*, 797 F.2d 1222 (2d Cir. 1986) (Comprehensiveness and complexity of the file structures within the program made the file structures sufficiently informative to warrant copyright protection); *CMAX/Cleveland, Inc. v. UCR, Inc.*, 804 F. Supp. 337 (M.D. Ga. 1992); *DVD Copy Control Association v. McLaughlin*, No. CV 786804, 2000 WL 48512 (Cal. Super. Jan. 21, 2000)
[91] Okanogan County Cause no. 00-1-0026-8
[92] *Frye v. United States*, 293 F. 1013 (D.C.Cir.1923)
[93] 90 Wash.App. 100; 950 P.2d 1024
[94] 2000 WL 288443 (W.D.Mich. 2000)
[95] Sonoma County, California Superior Ct. no SCR28424.
[96] *Frye v. United States*, *supra*.
[97] *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579, 113 S.Ct. 2786, 125 L.Ed.2d 469 (1993).
[98] *People v. Rodriguez* transcript of January 11, 2001 hearing, p 88, ln 27.

[99] See, e.g., *United States v. Liebert,* 519 F.2d 542, 547 (3rd Cir. 1975) (holding that computer evidence was admissible in criminal trial provided that prosecution lays a sufficient foundation to warrant a finding that such information is trustworthy and the defense is given the same opportunity to inquire into the accuracy of the computer system involved in producing such evidence). *United States v. Weatherspoon,* 581 F.2d 595, 598 (7th Cir. 1978) (same)
[100] *Horton v. California,* 496 U.S. 128, 134, 110 S.Ct. 2301, 2307, 110 L.Ed.2d 112 (1990)
[101] *United States v. Roberts*, 86 F.Supp.2d 678 (S.D.Tex 2000) (Warrantless search by Customs agents of the defendant's computer and zip disks constituted a routine export search, valid under the Fourth Amendment). This holding is specifically limited to border or export searches.
[102] *United States v. Turner* 169 F.3d 84 (1st Cir. 1999) (Suppressing all evidence obtained from a warrantless search of suspect's computer files), *United States v. Barth* 26 F.Supp.2d 929, 935-936 (D.C. Texas 1998) (same).
[103] *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999)
[104] U.S. Department of Justice*, Federal Guidelines for Searching and Seizing Computers* (1994) Note 12, at 89.
[105] *United States v. Hunter*, 13 F. Supp. 2d 574, 583 (D. Vt. 1998).
[106] 152 F.3d 1241 (10th Cir.1998)
[107] *United States v. Simpson, supra*, 153 F.2d at 1248.
[108] 168 F.3d 532 (1999)
[109] *United States v. Upham*, supra, 168 F.3d at 535
[110] *Id.* at 537.
[111] See *Davis v. Gracey*, 111 F.3d 1472, 1480 (10th Cir.1997) (upholding seizure of computer and all files contained therein because probable cause supported seizure of computer as an instrumentality of the crime); *United States v. Kimbrough,* 69 F.3d 723, 727 (5th Cir 1995) (upholding warrant allowing seizure of "hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media-floppy disks, CD ROMs, tape systems and hard drive, other computer related operational equipment ... used to visually depict a minor engaging in sexually explicit conduct"); *United States v. Lamb*, 945 F. Supp. 441, 457-58 (N.D.N.Y. 1996) (finding e-mail messages discussing the transport of child pornography to have a sufficient nexus to the crime and thus subject to seizure).
[112] 119 F.3d 742, 745 (9th Cir. 1997)
[113] 58 F.3d 423, 426 (9th Cir.1995)
[114] *United States v. Kow*, *supra*, 58 F.3d 423 at 427
[115] See *Marron v. United States*, 275 U.S. 192, 196, 47 S.Ct. 74, 76, 72 L.2d 231 (1927) (particularity requirement "prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.")
[116] 172 F.3d 1268 (10th Cir. 1999)
[117] *United States v. Carey*, *supra,* 172 F.3d at 1272-1273.
[118] *Id.,* at 1271
[119] *Id.*
[120] *Id.*
[121] *Id.* at 1272
[122] *Id.*
[123] *Id*. at 1274
[124] *Id.* at 1273
[125] *Id*. at 1275
[126] *Id*.,
[127] *Carey*, at 1275
[128] Id., citing, Raphael Winick, Searches and Seizures of Computers and Computer Data, 8 Harv. J.L. & Tech. 75, 104 (1994).
[129] The court notes: "Although the question of what constitutes 'plain view' in the context of computer files is intriguing and appears to be an issue of first impression for this court, and many others, we do not need to reach it here." *Carey,* at 1273.
[130] *Id.*
[131] Concurring opinion of Judge Baldock*, Carey*, at 1277

[132] 78 F.Supp.2d 524 (D.VA 1999)
[133] *United States v. Gray, supra*, 78 F.Supp.2d at 526
[134] *Id.* at 527.
[135] *Id.*
[136] *Id.*
[137] *Id*. at 528.
[138] *Id*. at 529, citing *United States v. Hunter, supra*, 13 F.Supp.2d at 584.
[139] *United States v. Gray*, supra, 78 F.Supp.2d at 530.
[140] *Id*. at 529.
[141] 2000 WL 288443 (W.D.Mich. 2000)
[142] 83 F.Supp.2d 187 (D.Mass 2000)
[143] *United States v. Scott, supra*, 183 F.Supp.2d at 195.
[144] *Id*. at 196.
[145] *Id*. at 197
[146] Although the opinion does not reflect the type of software utilized, *the EnCase Legal Journal* confirmed with the investigating agent identified in the opinion that EnCase was used for the investigation. (March 28, 2000 telephone interview of USSS Special Agent Bruce Rittenour).
[147] *United States v. Scott, supra*, 183 F.Supp.2d at 197-198
[148] 2000 WL 675942, Wisconsin Supreme Court Decision
[149] *supra*, 78 F.Supp.2d at 526
[150] *United States v. Brunnette* 76 F.Supp.2d 30 (D.ME 1999), citing, *Sgro v. United States*, 287 U.S. 206, 210, 53 S.Ct. 138, 140, 77 L.Ed. 260 (1932)
[151] *supra*, 76 F.Supp.2d at 42
[152] 36 F.3d 457, 462 (5th Cir. 1994)
[153] *supra*, 168 F.3d 532
[154] *supra*, 13 F.Supp.2d at 583
[155] 188 F.R.D. 111, 117 (1998 D.C. Cir)
[156] *Playboy Enterprises v. Welles*, 60 F.Supp.2d 1050, 1054 (S.D. CA 1999)
[157] 194 F.R.D. 639 (SD Ind. 2000)
[158] July 18, 2000 phone interview with Shawn Howell of Computer Forensics, Inc.
[159] 43 F.Supp.2d 951, 954 (E.D. Ill 1999)
[160] See, e.g., *Flagg Bros., Inc. v. Brooks*, 436 U.S. 149, 156 (1978) (stating that most constitutional rights "are protected only against infringement by governments"); *Jackson v. Metropolitan Edison Co*., 419 U.S. 345, 349 (1974) (describing "essential dichotomy" between deprivations of rights by state action and private conduct).
[161] See 18 U.S.C. §§ 1367, 2521, 3117, 3121-3127 (1994).
[162] Connecticut Public Act no. 98-142. There are exceptions under this statute where the employer has reasonable grounds to suspect that the employee is engaging in unlawful conduct or conduct creating a hostile workplace environment, and such monitoring may produce evidence of this misconduct.
[163] *Smyth v. Pillsbury Co*, 914 F.Supp. 97 (E.D. Pa. 1996)
[164] See, e.g. "Employer Liability for Employee Online Criminal Acts." *Federal Communications Law Journal*, (1999) 51 FCLJ 467
[165] See *Id*.
[166] (2000) 751 A.2d 538
[167] *Smyth v. Pillsbury Co*., *supra*, 914 F.Supp at 100.
[168] See 18 U.S.C. §§ 1367, 2521, 3117, 3121-3127 (1994).
[169] *Fraser v. Nationwide Mutual Insurance Co*. 135 F.Supp.2d 623, 636 (2001 D. Penn)
[170] Yochai Benkler, "Rules of the Road for the Information Superhighway" § 1, § 20.3[1] (1996) (discussing effects of ECPA's passage).
[171] See, e.g., Michael D. Scott et al., Scott on Multimedia Law § 12.04 [[A] (2d ed. Supp. 1997) (asserting that ECPA "would not apply to corporate or other 'non-public' computer networks.... [A] company's review of e-mail transmitted through or stored on its computer system would not violate the ECPA"); Kent D. Stuckey et al., Internet and Online Law § 5.03[1] (Release 2 1998) (stating that ECPA "does not ... protect against employers monitoring the e-mail of their employees").
[172] 18 U.S.C. §§ 2511(3)(a), 2702(a)(1) (1994).

[173] See 18 U.S.C. § 2701(c)(1) (1994) (exempting all "conduct authorized...by the person or entity providing a wire or electronic communications service"). The provider of electronic communications services is known as the "network provider."
[174] 932 F. Supp. 1232 (D. Nev. 1996)
[175] See *Id*. at 1232. The officers had used the police department's alphanumeric paging system to send messages to each other. See *Id*. at 1233. The contents of these messages led to an internal affairs investigation of the officers.
[176] See *Id*. at 1236
[177] *Steve Jackson Games, supra,* 36 F.3d at 463
[178] *Steve Jackson Games*, *supra,* 36 F.3d at 463 (holding that seizure of e-mail sent to bulletin board but not yet read by intended recipients did not constitute unlawful interception); *United States v. Reyes*, 922 F. Supp. 818, 836-37 (S.D.N.Y. 1996) (same).
[179] 135 F.Supp.2d 623 (2001 D. Penn)
[180] 2001 WL 576133 (2001 D.Mass)
[181] *Steve Jackson Games, supra,* 36 F.3d at 463
[182] See *Bohach,* 932 F. Supp. at 1235-36 ("The statutes therefore distinguish the 'interception' of an electronic communication at the time of transmission from the retrieval of such a communication after it has been put into 'electronic storage." '); *Reyes*, 922 F. Supp. at 836 ("[T]he definitions [in the ECPA] thus imply a requirement that the acquisition of the data be simultaneous with the original transmission of the data.").
[183] *Konop v. Hawaiian Airlines, Inc.* 236 F.3d 1035 (9th Cir.2001). A close examination of *Konop* reveals that it is clearly an "intermediate storage" case.
[184] See § 9.01
[185] California SB1016, sponsored by Debra Bowen, D-Redondo Beach.
[186] *Smyth v. Pillsbury Co*., *supra*, 914 F.Supp at 100 (recognizing the theoretical possibility of such a claim).
[187] See, e.g., Mike Causey, *Telecommuting Today*, Wash. Post, July 8, 1997, at B2 .
[188] See, e.g., H.G. Reza, *The Few, the Proud, the Online*, L.A. Times (Orange County ed.), Dec. 25, 1997, at E1, available in LEXIS, News Library, LAT File.
[189] *O'Connor v. Ortega*, 480 U.S. 709, 715, 107 S.Ct. 1492, 94 L.Ed.2d 714 (1987) (a plurality decision); *Shields v. Burge*, 874 F.2d 1201, 1203-04 (7th Cir.1989)
[190] *O'Connor*, 480 U.S. at 717, 107 S.Ct. 1492; id. at 737, 107 S.Ct. 1492 (Blackmun, J., dissenting).
[191] 206 F.3d 392 (4th Cir 2000)
[192] *Id*. at 398, fn. 9.
[193] *Id*. at 399-400.
[194] *United States v. Simons, supra*, 206 F.3d at 399, fn 10.
[195] *Id*. at 726, 107 S.Ct. 1492
[196] *Id*. (citing *New Jersey v. T.L.O.,* 469 U.S. 325, 342, 105 S.Ct. 733, (1985)).